Superelliptic curves with many automorphisms and CM Jacobians

Tony Shaska, Sr.

RISAT, Research Institute of Science and Technology,
9405, Vlorë, Albania.

March 20, 2022

Problem

Problem: Let $\mathcal{X}$ be a smooth, algebraic curve of genus $g \geq 1$, defined over a field k, and its Jacobian Jac $_k(\mathcal{X})$. Determine when Jac $\mathcal{X}$ has complex multiplication (CM).

They were first studied by M. Deuring (Deuring, 1941; 1949) for elliptic curves and generalized to Abelian varieties by (Shimura and Taniyama, 1961).

$\mathcal{X}$ is said to have complex multiplication when Jac $_k(\mathcal{X})$ is of CM-type.

CM is a property of the Jacobian, so it is an invariant of $\mathcal{X}$.

Is there anything special about the points in $\mathcal{M}_g$ for which Jac $_k(\mathcal{X})$ is of CM-type?

F. Oort asked if curves with *many automorphisms* are all of CM-type?

The answer to this question is negative.

In (Obus and Shaska, 2021) we focus on superelliptic curves and prove the following:

Theorem (Obus-Sh 2021)

If $\mathcal{X}$ is a superelliptic curve with many automorphisms, then $\mathcal{X}$ is one of the curves on the following Table and whether or not Jac $\mathcal{X}$ has CM is determined in column 6. $\mathcal{X}$ is has CM if and only if it is one of the cases in Table 1.

Nr.	$\overline{N}$	sig. $\overline{N}$	n	g	$f(x)$	CM?	Justification
$\mathcal{X}_0$	A_4	(2,3,3)	4	3	p_4	YES	Prop. ??
$\mathcal{X}_1$	A_4	(2,3,3)	2	4	$p_4 t_4$	YES	Prop. ??
$\mathcal{X}_2$			5	16		NO	Prop. ??
$\mathcal{X}_3$			10	36		NO	Cor. ??
$\mathcal{X}_4$	S_4	(2,4,4)	2	5	r_4	YES	Prop. ??
$\mathcal{X}_5$			3	10		NO	Prop. ??
$\mathcal{X}_6$			4	15		NO	Prop. ??
$\mathcal{X}_7$			6	25		NO	Cor. ??
$\mathcal{X}_8$			12	55		NO	Cor. ??
$\mathcal{X}_9$	S_4	(2,4,4)	2	3	s_4	NO	Prop. ??
$\mathcal{X}_{10}$			4	9		NO	Prop. ??
$\mathcal{X}_{11}$			8	21		NO	Prop. ??
$\mathcal{X}_{12}$	S_4	(2,4,4)	2	2	t_4	YES	Prop. ??
$\mathcal{X}_{13}$			3	4		YES	Prop. ??
$\mathcal{X}_{14}$			6	10		YES	Prop. ??
$\mathcal{X}_{15}$	S_4	(2,4,4)	2	9	$r_4 s_4$	NO	Prop. ??
$\mathcal{X}_{16}$			4	27		NO	Prop. ??
$\mathcal{X}_{17}$			5	36		NO	Prop. ??
$\mathcal{X}_{18}$			10	81		NO	Prop. ??
$\mathcal{X}_{19}$			20	171		NO	Prop. ??
$\mathcal{X}_{20}$	S_4	(2,4,4)	2	8	$r_4 t_4$	YES	Prop. ??
$\mathcal{X}_{21}$			3	16		NO	Prop. ??
$\mathcal{X}_{22}$			6	40		NO	Cor. ??
$\mathcal{X}_{23}$			9	64		NO	Cor. ??
$\mathcal{X}_{24}$			18	136		NO	Cor. ??
$\mathcal{X}_{25}$	S_4	(2,4,4)	2	6	$s_4 t_4$	NO	Prop. ??
$\mathcal{X}_{26}$			7	36		NO	Prop. ??
$\mathcal{X}_{27}$			14	78		NO	Prop. ??
$\mathcal{X}_{28}$	S_4	(2,4,4)	2	12	$r_4 s_4 t_4$	NO	Prop. ??
$\mathcal{X}_{29}$			13	144		NO	Prop. ??
$\mathcal{X}_{30}$			26	300		NO	Prop. ??
$\mathcal{X}_{31}$	A_5	(2,3,5)	2	9	r_5	NO	Prop. ??
$\mathcal{X}_{32}$			4	27		NO	Prop. ??
$\mathcal{X}_{33}$			5	36		NO	Prop. ??
$\mathcal{X}_{34}$			10	81		NO	Prop. ??
$\mathcal{X}_{35}$			20	171		NO	Prop. ??
$\mathcal{X}_{36}$	A_5	(2,3,5)	2	5	s_5	NO	Prop. ??
$\mathcal{X}_{37}$			3	10		YES	Prop. ??
$\mathcal{X}_{38}$			4	15		NO	Prop. ??
$\mathcal{X}_{39}$			6	25		NO	Prop. ??

$\mathcal{X}_{40}$			12	55		NO	Prop. **??**
$\mathcal{X}_{41}$	A_5	(2,3,5)	2	14	t_5	YES	Prop. **??**
$\mathcal{X}_{42}$			3	28		NO	Prop. **??**
$\mathcal{X}_{43}$			5	56		NO	Prop. **??**
$\mathcal{X}_{44}$			6	70		NO	Cor. **??**
$\mathcal{X}_{45}$			10	126		NO	Cor. **??**
$\mathcal{X}_{46}$			15	196		NO	Cor. **??**
$\mathcal{X}_{47}$			30	406		NO	Cor. **??**
$\mathcal{X}_{48}$	A_5	(2,3,5)	2	15	$r_5 s_5$	NO	Prop. **??**
$\mathcal{X}_{49}$			4	45		NO	Prop. **??**
$\mathcal{X}_{50}$			8	105		NO	Prop. **??**
$\mathcal{X}_{51}$			16	225		NO	Prop. **??**
$\mathcal{X}_{52}$			32	465		NO	Prop. **??**
$\mathcal{X}_{53}$	A_5	(2,3,5)	2	24	$r_5 t_5$	NO	Prop. **??**
$\mathcal{X}_{54}$			5	96		NO	Prop. **??**
$\mathcal{X}_{55}$			10	216		NO	Prop. **??**
$\mathcal{X}_{56}$			25	576		NO	Cor. **??**
$\mathcal{X}_{57}$			50	1176		NO	Prop. **??**
$\mathcal{X}_{58}$	A_5	(2,3,5)	2	20	$s_5 t_5$	NO	Prop. **??**
$\mathcal{X}_{59}$			3	40		NO	Prop. **??**
$\mathcal{X}_{60}$			6	100		NO	Prop. **??**
$\mathcal{X}_{61}$			7	120		NO	Prop. **??**
$\mathcal{X}_{62}$			14	260		NO	Prop. **??**
$\mathcal{X}_{63}$			21	400		NO	Cor. **??**
$\mathcal{X}_{64}$			42	820		NO	Prop. **??**
$\mathcal{X}_{65}$	A_5	(2,3,5)	2	30	$r_5 s_5 t_5$	NO	Prop. **??**
$\mathcal{X}_{66}$			31	900		NO	Prop. **??**
$\mathcal{X}_{67}$			62	1830		NO	Prop. **??**

Next we will explain what the results of the table mean and give an outline of the proof.

Abelian varieties I

Group schemes: A projective (affine) group scheme G defined over k is a projective (affine) scheme over k endowed with

- addition, i.e., a morphism $m: \; G \times G \rightarrow G$
- inverse, i.e., a morphism $i: \; G \rightarrow G$
- the identity, i. e., a k-rational point $0 \in G(k)$,

such that it satisfies group laws.

An **Abelian variety** (over k) is an absolutely irreducible projective variety defined over k which is a group scheme. A morphism of Abelian varieties $\phi : \mathcal{A} \rightarrow \mathcal{B}$ is a **homomorphism** which maps the identity element of $\mathcal{A}$ to the identity element of $\mathcal{B}$. $\mathcal{A}/k$ is called **simple** if it has no proper non-zero Abelian subvariety over k and **absolutely simple** (or **geometrically simple**) if it is simple over $\bar{k}$.

The $\mathbb{Z}$-module of homomorphisms $\mathcal{A} \mapsto \mathcal{B}$ is denoted by $\mathrm{Hom}(\mathcal{A}, \mathcal{B})$ and the ring of endomorphisms $\mathcal{A} \mapsto \mathcal{A}$ by $\mathrm{End}\,\mathcal{A}$. It's more convenient to work with $\mathbb{Q}$-vector spaces

$$\mathrm{Hom}^0(\mathcal{A}, \mathcal{B}) := \mathrm{Hom}(\mathcal{A}, \mathcal{B}) \otimes_{\mathbb{Z}} \mathbb{Q}, \quad \text{and } \mathrm{End}^{\,0}\mathcal{A} := \mathrm{End}\,\mathcal{A} \otimes_{\mathbb{Z}} \mathbb{Q}.$$

Lemma: If there exists an algorithm to compute $\mathrm{End}_{\,K}(\mathcal{A})$ for $\dim \mathcal{A} \geq 1$ defined over a number field K, then there is an algorithm to compute $\mathrm{End}_{\,\bar{K}}(\mathcal{A})$.

The ring of endomorphisms of generic Abelian varieties is "as small as possible". For instance, if $\mathrm{char}(k) = 0$ $\mathrm{End}\,(\mathcal{A}) = \mathbb{Z}$ in general. If k is a finite field, the Frobenius endomorphism will generate a larger ring, but again, this will be all in the generic case.

Abelian varieties with complex multiplication I

End $^0(\mathcal{A})$ is a $\mathbb{Q}$-algebra of dimension $\leq 4\dim(\mathcal{A})^2$. End $^0(\mathcal{A})$ is a semi-simple algebra (a complete classification due to Albert of *possible* algebra structures on End $^0(\mathcal{A})$).

$\mathcal{A}$ has complex multiplication over a field K if End $^0_K(\mathcal{A})$ contains a commutative, semisimple $\mathbb{Q}$-algebra of dimension $2\dim\mathcal{A}$.

Question: Which algebras occur as endomorphism algebras? Well understood in char$(k) = 0$ (due to Albert), but wide open in char $= p > 0$.

Theorem (Deuring)

Let $\mathcal{E}$ be an elliptic curve defined over a field k. The following hold:

i) *If char$(k) = 0$, then $\mathcal{E}$ is ordinary and End $_{\bar{k}}(\mathcal{E}) = \mathbb{Z}$ (generic case) or End $_{\bar{k}}(\mathcal{E})$ is an order $O_{\mathcal{E}} \subset \mathbb{Q}(\sqrt{-d_{\mathcal{E}}})$, $d_{\mathcal{E}} > 0$ (CM-case).*

ii) *(**Deuring's Lifting Theorem**) Let $\mathcal{E}$ be over $\mathbb{F}_q$ which is ordinary over $\overline{\mathbb{F}_q}$. Then there is, up to $\mathbb{C}$-isomorphisms, exactly one elliptic curve $\tilde{\mathcal{E}}$ with CM over a number field K such that*

- *there is a prime $\mathfrak{p}$ of K with $\tilde{\mathcal{E}}_{\mathfrak{p}} \cong \mathcal{E}$ with $\tilde{\mathcal{E}}_{\mathfrak{p}}$ the reduction of $\tilde{\mathcal{E}}$ modulo $\mathfrak{p}$, and*
- *End $(\tilde{\mathcal{E}}) =$ End $(\mathcal{E})_{\mathfrak{p}} = O_{\mathcal{E}}$, with $O_{\mathcal{E}}$ an order in an imaginary quadratic field.*

iii) *If $\mathcal{E}$ is supersingular, then*

- *all supersingular elliptic curves in characteristic p are defined over $\mathbb{F}_{p^2}$, (up to twists,) i.e. their j-invariant lies in $\mathbb{F}_{p^2}$.*
- *$|\mathcal{E}(\mathbb{F}_{p^2})| = (p \pm 1)^2$, and the sign depends on the twist class of $\mathcal{E}$.*
- *End $_{\overline{\mathbb{F}_p}}(\mathcal{E})$ is a maximal order in the quaternion algebra $\mathbb{Q}_p$, unramified outside $\{\infty, p\}$.*

Jacobian varieties

Can we say anything for higher dimensional Jacobian varieties?

If a curve $\mathcal{C}$ has non-trivial automorphisms then it has a bigger chance to have $\text{End}_K^0(\text{Jac}\,\mathcal{C})$ larger than $\mathbb{Z}$ and therefore have CM.

This was the main reasoning behind Ort's first guess that curves with many automorphisms might have CM Jacobians. Such curves must correspond to special points in the moduli space of curves. It is still not clear how one can characterize such moduli points.

The following is the best general condition for a curve $\mathcal{X}$ to have CM Jacobian.

Let $\chi_{\mathcal{C}}$ be the character of the representation of G on $H^0(\mathcal{C}, \Omega_{\mathcal{C}})$, $\text{Sym}^2 \chi_{\mathcal{C}}$ the character of G on $\text{Sym}^2_{\mathbb{C}} H^0(\mathcal{C}, \Omega_{\mathcal{C}})$, χ_{triv} the trivial representation on $\mathbb{C}$.

Theorem (Streit 2001)
If $\langle Sym^2 \chi_{\mathcal{C}}, \chi_{triv} \rangle = 0$, then Jac $\mathcal{C}$ has complex multiplication; (Streit, 2001).

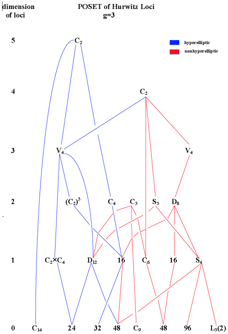
Next we will focus on curves with many automorphisms as defined by Ort.

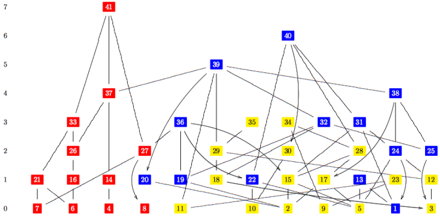
Curves with many automorphisms I

Let $\mathcal{C}$ be e genus $g \geq 2$ curve over $k = \bar{k}$, $\mathfrak{p} \in \mathcal{M}_g$ its moduli point, and $G := \mathrm{Aut}_k(\mathcal{C})$.

$\mathcal{C}$ has **many automorphisms** if $\mathfrak{p} \in \mathcal{M}_g$ has a neighborhood U such that all curves corresponding to points in $U \setminus \{\mathfrak{p}\}$ have automorphism group strictly smaller than $\mathfrak{p}$. The following are equivalent:

1. $\mathcal{C}$ has many automorphisms
2. There exists $H < G$ s.t. $g(\mathcal{C}/H) = 0$ and $\mathcal{C} \to \mathcal{C}/H$ has at most 3 branch points.
3. The quotient $\mathcal{C}/G$ has genus 0 and $\mathcal{C} \to \mathcal{C}/G$ has at most three points.
4. Let σ be the signature of $\mathcal{C} \to \mathcal{C}/G$. Then $\mathcal{C}$ has many automorphisms if and only if $g(\mathcal{C}/G) = 0$ and the moduli dimension of the Hurwitz space $\mathcal{H}(g, G, \sigma)$ is 0.





Curves with many automorphisms II

A **superelliptic curve** is a smooth projective curve $\mathcal{X}$ of genus ≥ 2 with affine equation $y^n = \prod_{i=1}^{r}(x - a_i)$, with the a_i distinct complex numbers such that there is a cyclic subgroup $H := \langle \tau \rangle \leq G$, where $\tau(y) = \zeta_n y$

(i) If H is as above, then H is *normal* in $G := \mathrm{Aut}(\mathcal{X})$.

(ii) Either $n \mid r$ or $\gcd(n, r) = 1$ (this guarantees that all branch points have index n).

If $\mathcal{X}$, H, and τ are as above, we call τ a superelliptic automorphism (of level n) and H a superelliptic group (of level n) of $\mathcal{X}$. Let $\pi : \mathcal{X} \to \mathbb{P}^1 = \mathcal{X}/H$ be H-cover. There is a short exact sequence

$$1 \to H \to G \to \overline{G} \to 1,$$

where $\overline{G} := G/h \hookrightarrow \mathrm{PGL}_2(\mathbb{C})$. $\overline{G}$ is called the reduced automorphism group of $\mathcal{X}$.

A pre-superelliptic curve to be a curve satisfying all the requirements of a superelliptic curve except possibly for (i) above. Let $N = N_G(H)$ be the normalizer of H in G, then we have a similar exact sequence $1 \to H \to N \to \overline{N} \to 1$, and we call $\overline{N}$ the **reduced automorphism group** of $\mathcal{X}$. In this case, H is called a pre-superelliptic group and τ is called a pre-superelliptic automorphism.

Because verifying that a curve is pre-superelliptic does not depend on computing its entire automorphism group, it can be significantly easier than verifying that a curve is superelliptic. This is why we work with pre-superelliptic curves throughout the talk.

Theorem ((Sanjeewa and Shaska, 2008))

Let char $k = p \neq 2, 3, 5$. Groups G, $\bar{G}$, signatures of $\mathcal{C} \to \mathcal{C}/G$, mod. dimension, and parametric eqs. of $\mathcal{C}$ are:

#	G	$\delta(G,C)$	δ, n, g	$\mathcal{C} = (C_1, ..., C_r)$
1	$(p,m)=1$	$\frac{2(g+n-1)}{m(n-1)} - 1$	$n < g+1$	$(m, m, n, ..., n)$
2	C_m	$\frac{2g+n-1}{m(n-1)} - 1$		$(m, mn, n, ..., n)$
3		$\frac{2g}{m(n-1)} - 1$	$n < g$	$(mn, mn, n, ..., n)$
4	$(p,m)=1$	$\frac{g+n-1}{m(n-1)}$		$(2, 2, m, n, ..., n)$
5		$\frac{2g+m+2n-nm-2}{2m(n-1)}$		$(2n, 2, m, n, ..., n)$
6	D_{2m}	$\frac{g}{m(n-1)}$		$(2, 2, mn, n, ..., n)$
7		$\frac{g+m+n-mn-1}{m(n-1)}$	$n < g+1$	$(2n, 2n, m, n, ..., n)$
8		$\frac{2g+m-mn}{2m(n-1)}$	$g \neq 2$	$(2n, 2, mn, n, ..., n)$
9		$\frac{g+m-mn}{m(n-1)}$	$n < g$	$(2n, 2n, mn, n, ..., n)$
10		$\frac{n+g-1}{6(n-1)}$		$(2, 3, 3, n, ..., n)$
11	A_4	$\frac{g-n+1}{6(n-1)}$		$(2, 3n, 3, n, ..., n)$
12		$\frac{g-3n+3}{6(n-1)}$		$(2, 3n, 3n, n, ..., n)$
13		$\frac{g-2n+2}{6(n-1)}$	$\delta \neq 0$	$(2n, 3, 3, n, ..., n)$
14		$\frac{g-4n+4}{6(n-1)}$		$(2n, 3n, 3, n, ..., n)$
15		$\frac{g-6n+6}{6(n-1)}$	$\delta \neq 0$	$(2n, 3n, 3n, n, ..., n)$
16		$\frac{g+n-1}{12(n-1)}$		$(2, 3, 4, n, ..., n)$
17		$\frac{g-3n+3}{12(n-1)}$		$(2, 3n, 4, n, ..., n)$
18		$\frac{g-2n+2}{12(n-1)}$		$(2, 3, 4n, n, ..., n)$
19		$\frac{g-6n+6}{12(n-1)}$		$(2, 3n, 4n, n, ..., n)$
20	S_4	$\frac{g-5n+5}{12(n-1)}$		$(2n, 3, 4, n, ..., n)$
21		$\frac{g-9n+9}{12(n-1)}$		$(2n, 3n, 4, n, ..., n)$
22		$\frac{g-8n+8}{12(n-1)}$		$(2n, 3, 4n, n, ..., n)$
23		$\frac{g-12n+12}{12(n-1)}$		$(2n, 3n, 4n, n, ..., n)$
24		$\frac{g+n-1}{30(n-1)}$		$(2, 3, 5, n, ..., n)$
25		$\frac{g-5n+5}{30(n-1)}$		$(2, 3, 5n, n, ..., n)$
26		$\frac{g-15n+15}{30(n-1)}$		$(2, 3n, 5n, n, ..., n)$
27		$\frac{g-9n+9}{30(n-1)}$		$(2, 3n, 5, n, ..., n)$
28	A_5	$\frac{g-14n+14}{30(n-1)}$		$(2n, 3, 5, n, ..., n)$
29		$\frac{g-20n+20}{30(n-1)}$		$(2n, 3, 5n, n, ..., n)$
30		$\frac{g-24n+24}{30(n-1)}$		$(2n, 3n, 5, n, ..., n)$
31		$\frac{g-30n+30}{30(n-1)}$		$(2n, 3n, 5n, n, ..., n)$
32		$\frac{2g+2n-2}{p^t(n-1)} - 2$		$(p^t, n, ..., n)$
33	U	$\frac{2g+np^t-p^t}{p^t(n-1)} - 2$	$(n,p)=1, n \mid p^t-1$	$(np^t, n, ..., n)$
34		$\frac{2(g+n-1)}{mp^t(n-1)} - 1$	$(m,p)=1, m \mid p^t-1$	$(mp^t, m, n, ..., n)$
35		$\frac{2g+2n+p^t-np^t-2}{mp^t(n-1)} - 1$	$(m,p)=1, m \mid p^t-1$	$(mp^t, nm, n, ..., n)$
36	K_m	$\frac{2g+np^t-p^t}{mp^t(n-1)} - 1$	$(nm,p)=1, nm \mid p^t-1$	$(nmp^t, m, n, ..., n)$
37		$\frac{2g}{mp^t(n-1)} - 1$	$(nm,p)=1, nm \mid p^t-1$	$(nmp^t, nm, n, ..., n)$
38		$\frac{2(g+n-1)}{m(n-1)} - 1$	$\left(\frac{q-1}{2}, p\right) = 1$	$(\alpha, \beta, n, ..., n)$
39	$PSL_2(q)$	$\frac{2g+q(q-1)-n(q+1)(q-2)-2}{m(n-1)} - 1$	$\left(\frac{q-1}{2}, p\right) = 1$	$(\alpha, n\beta, n, ..., n)$
40		$\frac{2g+nq(q-1)+q-q^2}{m(n-1)} - 1$	$\left(\frac{n(q-1)}{2}, p\right) = 1$	$(n\alpha, \beta, n, ..., n)$
41		$\frac{2g}{m(n-1)} - 1$	$\left(\frac{n(q-1)}{2}, p\right) = 1$	$(n\alpha, n\beta, n, ..., n)$
42		$\frac{2(g+n-1)}{m(n-1)} - 1$	$(q-1, p) = 1$	$(2\alpha, 2\beta, n, ..., n)$
43	$PGL_2(q)$	$\frac{2g+q(q-1)-n(q+1)(q-2)-2}{m(n-1)} - 1$	$(q-1, p) = 1$	$(2\alpha, 2n\beta, n, ..., n)$
44		$\frac{2g+nq(q-1)+q-q^2}{m(n-1)} - 1$	$(n(p-1), p) = 1$	$(2n\alpha, 2\beta, n, ..., n)$
45		$\frac{2g}{m(n-1)} - 1$	$(n(q-1), p) = 1$	$(2n\alpha, 2n\beta, n, ..., n)$

#	$\bar{G}$	$y^n = f(x)$
1		$x^{m\delta} + a_1 x^{m(\delta-1)} + \cdots + a_\delta x^m + 1$
2	C_m	$x^{m\delta} + a_1 x^{m(\delta-1)} + \cdots + a_\delta x^m + 1$
3		$x(x^{m\delta} + a_1 x^{m(\delta-1)} + \cdots + a_\delta x^m + 1)$
4		$F(x) := \prod_{i=1}^{\delta}(x^{2m} + \lambda_i x^m + 1)$
5		$(x^m - 1) \cdot F(x)$
6		$x \cdot F(x)$
7	D_{2m}	$(x^{2m} - 1) \cdot F(x)$
8		$x(x^m - 1) \cdot F(x)$
9		$x(x^{2m} - 1) \cdot F(x)$
10		$G(x) := \prod_{i=1}^{\delta}(x^{12} - \lambda_i x^{10} - 33x^8 + 2\lambda_i x^6 - 33x^4 - \lambda_i x^2 + 1)$
11		$(x^4 + 2i\sqrt{3}x^2 + 1) \cdot G(x)$
12	A_4	$(x^8 + 14x^4 + 1) \cdot G(x)$
13		$x(x^4 - 1) \cdot G(x)$
14		$x(x^4 - 1)(x^4 + 2i\sqrt{3}x^2 + 1) \cdot G(x)$
15		$x(x^4 - 1)(x^8 + 14x^4 + 1) \cdot G(x)$
16		$M(x)$
17		$S(x) \cdot M(x)$
18		$T(x) \cdot M(x)$
19		$S(x) \cdot T(x) \cdot M(x)$
20	S_4	$R(x) \cdot M(x)$
21		$R(x) \cdot S(x) \cdot M(x)$
22		$R(x) \cdot T(x) \cdot M(x)$
23		$R(x) \cdot S(x) \cdot T(x).M(x)$
24		$\Lambda(x)$
25		$(x(x^{10} + 11x^5 - 1)) \cdot \Lambda(x)$
26		$(x^{20} - 228x^{15} + 494x^{10} + 228x^5 + 1)(x(x^{10} + 11x^5 - 1)) \cdot \Lambda(x)$
27		$(x^{20} - 228x^{15} + 494x^{10} + 228x^5 + 1) \cdot \Lambda(x)$
28	A_5	$Q(x) \cdot \Lambda(x)$
29		$x(x^{10} + 11x^5 - 1).\psi(x) \cdot \Lambda(x)$
30		$(x^{20} - 228x^{15} + 494x^{10} + 228x^5 + 1) \cdot \psi(x) \cdot \Lambda(x)$
31		$(x^{20} - 228x^{15} + 494x^{10} + 228x^5 + 1)(x(x^{10} + 11x^5 - 1)) \cdot \psi(x) \cdot \Lambda(x)$
32	U	$B(x)$
33		$B(x)$
34		$\Theta(x)$
35	K_m	$x\prod_{j=1}^{\frac{p^t-1}{m}} (x^m - b_j) \cdot \Theta(x)$
36		$\Theta(x)$
37		$x\prod_{j=1}^{\frac{p^t-1}{m}} (x^m - b_j) \cdot \Theta(x)$
38		$\Delta(x)$
39	$PSL_2(q)$	$((x^q - x)^{q-1} + 1) \cdot \Delta(x)$
40		$(x^q - x) \cdot \Delta(x)$
41		$(x^q - x)((x^q - x)^{q-1} + 1) \cdot \Delta(x)$
42		$\Omega(x)$
43	$PGL_2(q)$	$((x^q - x)^{q-1} + 1) \cdot \Omega(x)$
44		$(x^q - x) \cdot \Omega(x)$
45		$(x^q - x)((x^q - x)^{q-1} + 1) \cdot \Omega(x)$

TABLE 4. The equations of the curves related to the cases in Table 2

Pre-superelliptic curves with many automorphisms

A pre-superelliptic curve $\mathcal{X}$ **has property ($\star$) with respect to** H if $\mathcal{X} \to \mathcal{X}/N$ is branched at exactly three points.

Proposition

Let $\mathcal{X}$ be a pre-superelliptic curve, H a pre-superelliptic group of level n, $N = N_G(H)$, and $\overline{N} = N/H$. Then $\overline{N}$ is isomorphic to either C_m, D_{2m}, A_4, S_4, or A_5. If $\mathcal{X}$ has property ($\star$), then furthermore:

(i) *If $\overline{N} \cong C_m$ then $\mathcal{X}$ has equation $y^n = x^m + 1$ or $y^n = x(x^m + 1)$.*

(ii) *If $\overline{N} \cong D_{2m}$ then $\mathcal{X}$ has equation $y^n = x^{2m} - 1$ or $y^n = x(x^{2m} - 1)$.*

(iii) *If $\overline{N} \cong A_4$ then $\mathcal{X}$ has equation $y^n = f(x)$ where*

$$f(x) = x^4 + 2i\sqrt{3}x^2 + 1 \text{ or } f(x) = x(x^4 - 1)(x^4 + 2i\sqrt{3}x^2 + 1).$$

Furthermore, the A_4-orbit of ∞ consists of itself and the roots of $x(x^4 - 1)$.

(iv) *If $\overline{N} \cong S_4$ then $\mathcal{X}$ has equation $y^n = f(x)$ where $f(x)$ is one of the following: $r_4(x)$, $s_4(x)$, $t_4(x)$, $r_4(x)s_4(x)$, $r_4(x)t_4(x)$, $s_4(x)t_4(x)$, $r_4(x)s_4(x)t_4(x)$, where*

$$r_4(x) = x^{12} - 33x^8 - 33x^4 + 1,\ s_4(x) = x^8 + 14x^4 + 1,\ t_4(x) = x(x^4 - 1).$$

Furthermore, the S_4-orbit of ∞ consists of itself and the roots of $t_4(x)$.

(v) *If $\overline{N} \cong A_5$ then $\mathcal{X}$ has equation $y^n = f(x)$ where $f(x)$ is one of the following: $r_5(x)$, $s_5(x)$, $t_5(x)$, $r_5(x)s_5(x)$, $r_5(x)t_5(x)$, $s_5(x)t_5(x)$, $r_5(x)s_5(x)t_5(x)$, where*

$$r_5(x) = x^{20} - 228x^{15} + 494x^{10} + 228x^5 + 1$$
$$s_5(x) = x(x^{10} + 11x^5 - 1)$$
$$t_5(x) = x^{30} + 522x^{25} - 10005x^{20} - 10005x^{10} - 522x^5 + 1.$$

Furthermore, the A_5-orbit of ∞ consists of itself and the roots of $s_5(x)$.

Hyperelliptic Jacobians with CM

Theorem:(Muller-Pink) Let $\mathcal{X}$ be hyperelliptic, $\alpha \in G$, $\bar{\alpha} \in \bar{G}$, $|\bar{\alpha}| = n$, P be a fixed point of $\bar{\alpha}$ in $\mathbb{P}^1_{\mathbb{C}}$, ξ the eigenvalue of $\bar{\alpha}$ on the tangent space at P. $k := 1$ if $P \in Br(\pi)$, $k := 0$ otherwise. Then,

$$\frac{1}{2}g(g+1) \text{ if } n = 1, \quad (-1)^k \frac{1}{4}\left(1 + (-1)^{g+1} + 2g\right) \text{ if } n = 2, \quad \xi^{2-k}\frac{(\xi^g - 1)(\xi^{g+1} - 1)}{(\xi - 1)(xi^2 - 1)} \text{ if } n > 2.$$

X	$\bar{G}$	Genus	Affine equation	G	Jac(X) has
X_1	C_{2g+1}	$g \geqslant 2$	$y^2 = x^{2g+1} - 1$	C_{4g+2}	CM
X_2	D_{2g+2}	$g \geqslant 2$	$y^2 = x^{2g+2} - 1$	V_{2g+2}	CM
X_3	D_{2g}	$g \geqslant 3$	$y^2 = x^{2g+1} - x$	U_{2g}	CM
X_4	A_4	4	$y^2 = t_4 p_4$	$\mathrm{SL}_2(3)$	CM
X_5	S_4	2	$y^2 = t_4$	$\mathrm{GL}_2(3)$	CM
X_6	S_4	3	$y^2 = s_4$	$C_2 \times S_4$	no CM
X_7	S_4	5	$y^2 = r_4$	W_2	CM
X_8	S_4	6	$y^2 = s_4 t_4$	$\mathrm{GL}_2(3)$	no CM
X_9	S_4	8	$y^2 = r_4 t_4$	W_3	CM
X_{10}	S_4	9	$y^2 = r_4 s_4$	W_2	no CM
X_{11}	S_4	12	$y^2 = r_4 s_4 t_4$	W_3	no CM
X_{12}	A_5	5	$y^2 = s_5$	$C_2 \times A_5$	no CM
X_{13}	A_5	9	$y^2 = r_5$	$C_2 \times A_5$	no CM
X_{14}	A_5	14	$y^2 = t_5$	$\mathrm{SL}_2(5)$	CM
X_{15}	A_5	15	$y^2 = r_5 s_5$	$C_2 \times A_5$	no CM
X_{16}	A_5	20	$y^2 = s_5 t_5$	$\mathrm{SL}_2(5)$	no CM
X_{17}	A_5	24	$y^2 = r_5 t_5$	$\mathrm{SL}_2(5)$	no CM
X_{18}	A_5	30	$y^2 = r_5 s_5 t_5$	$\mathrm{SL}_2(5)$	no CM

Table 1: All hyperelliptic curves with many automorphisms

Superelliptic curves with CM I

Lemma: If $\mathcal{X}$ is the quotient of a Fermat curve then Jac $(\mathcal{X})$ has CM.

Theorem: Suppose $\mathcal{X}$ is a pre-superelliptic curve with property $(\star)$. If $\overline{N}$ is cyclic or dihedral then Jac $(\mathcal{X})$ has CM.

If $\mathcal{X}$ has many automorphisms, then Jac $\mathcal{X}$ lies in a special subvariety of $\mathcal{A}_g$ of dim. $\langle \mathrm{Sym}^2 \chi_{\mathcal{X}}, \chi_{triv} \rangle$, see (Frediani et al., 2015). Since special subvarieties of dimension zero are CM points, Streit's criterion holds.

For higher dimension these subvarieties must contain CM points, but they may also contain non-CM points, so one can't conclude anything when Streit's criterion fails.

Let $\mathcal{X}$ be pre-superelliptic. For $\sigma \in N$, let $\bar{\sigma}$ for the image of σ in $\overline{N}$. We may consider $\mathrm{Sym}^2 \chi_{\mathcal{X}}$ as an N-representation. Recall a basic result of representation theory.

$$\mathrm{Sym}^2 \chi_{\mathcal{X}}(\sigma) = \frac{1}{2} \left(\chi_{\mathcal{X}}(\sigma^2) + \chi_{\mathcal{X}}(\sigma)^2 \right).$$

Superelliptic curves with CM II

Prop: For each $\overline{\sigma} \in \overline{N} \hookrightarrow \mathrm{PGL}_2(\mathbb{C})$, let $m = |\overline{\sigma}|$ and $\zeta_{\overline{\sigma}}$ be either ratio of the eigenvalues and $k_{\overline{\sigma}} = 1$ if $\overline{\sigma}$ fixes a branch point of $\mathcal{X} \to \mathbb{P}^1$ and $k_{\overline{\sigma}}0$ otherwise. Let ζ_n, be a primitive nth root of unity, and let $\zeta_{n,\overline{\sigma}}$ be a primitive mnth root of unity such that $\zeta_{n,\overline{\sigma}}^n = \zeta_{\overline{\sigma}}$. Let A be the set of ordered pairs defined below in Eq. **??**. If

$$\sum_{\overline{\sigma}\in\overline{N}} \sum_{i=0}^{n-1} \left(\sum_{(a,b)\in A} \zeta_{\overline{\sigma}}^{2(a+1)} \zeta_n^{2(b+1)i} \zeta_{n,\overline{\sigma}}^{2(b-n+1)k_{\overline{\sigma}}} + \left(\sum_{(a,b)\in A} \zeta_{\overline{\sigma}}^{a+1} \zeta_n^{(b+1)i} \zeta_{n,\overline{\sigma}}^{(b-n+1)k_{\overline{\sigma}}} \right)^2 \right)$$

vanishes, then $\mathcal{X}$ has CM.

Lemma: The curves $\mathcal{X}_1$, $\mathcal{X}_4$, $\mathcal{X}_{12}$, $\mathcal{X}_{13}$, $\mathcal{X}_{14}$, $\mathcal{X}_{20}$, $\mathcal{X}_{37}$, $\mathcal{X}_{41}$ all have CM. Curves $\mathcal{X}_1$, $\mathcal{X}_4$, $\mathcal{X}_{12}$, $\mathcal{X}_{20}$, and $\mathcal{X}_{41}$ are all hyperelliptic, and Streit's criterion was already verified for them in (Müller and Pink, 2017).

Proposition: Let $\mathcal{X}$ be a pre-superelliptic curve with property $(\star)$, and assume that $\overline{N} = C_m$ or D_{2m}. Then $\mathcal{X}$ satisfies Streit's criterion. That is, $\langle \mathrm{Sym}^2 \chi_{\mathcal{X}}, \chi_{triv} \rangle = 0$.

This gives another proof of the above Theorem.

Negative CM results I

Next we show that the remaining curves in Table 1 do not have CM.

Lemma: None of the curves $\mathcal{X}_i$ for i= 9, 10, 11, 15, 16, 18, 19, 25, 27, 28, 30, 31, 32, 34, 35, 36, 38, 39, 40, 48, 49, 50, 51, 52, 53, 55, 57, 58, 60, 62, 64, 65, 67 has CM, since they are either hyperelliptic or have quotients with no CM.

Using stable reduction:
Let $\mathcal{X} \to \mathbb{P}^1_K$ be the cover of $\mathbb{P}^1_K$ given by $y^n = \prod_i (x - \alpha_i)$, where the α_i are pairwise distinct elements of K and B be the set of branch points.

Let $\mathcal{Y}^{st}$ be the stable model of the marked curve $(\mathbb{P}^1_K, B)$, and let $\Gamma_{\overline{\mathcal{Y}}}$ be the dual graph of its special fiber. Assume that $g(\mathcal{X}) \geq 2$, which in turn implies $|B| \geq 3$.

There exists a finite extension L/K with valuation ring $\mathcal{O}_L$, such that the normalization of $\mathcal{Y}^{st} \times_{\mathcal{O}_K} \mathcal{O}_L$ in $L(\mathcal{X})$ is a semistable model of $\mathcal{X}$ over L. This induces a map of graphs $\pi : \Gamma_{\overline{\mathcal{X}}} \to \Gamma_{\overline{\mathcal{Y}}}$.

- **(i)** If v is a leaf of $\Gamma_{\overline{\mathcal{Y}}}$ (i.e., a vertex incident to only one edge), then $|\pi^{-1}(v)| \leq n/2$.
- **(ii)** Suppose there exists an edge e of $\Gamma_{\overline{\mathcal{Y}}}$ such that removing e splits $\Gamma_{\overline{\mathcal{Y}}}$ into two trees T_1 and T_2 where n divides the number of elements of B specializing to each of T_1 and T_2. Then $|\pi^{-1}(e)| = n$.

Negative CM results II

Prop: In the situation of (ii), the graph $\Gamma_{\overline{\mathcal{X}}}$ is not a tree. The curves $\mathcal{X}_{17}$, $\mathcal{X}_{21}$, $\mathcal{X}_{42}$, $\mathcal{X}_{54}$, $\mathcal{X}_{59}$, or $\mathcal{X}_{61}$ have no CM Jacobian.

For $\mathcal{X}_{61}$, the tree $\Gamma_{\overline{\mathcal{Y}}}$ for reduction modulo 5 is shown in (Mueller, 2017). In this case, $n = 7$, and there are four edges which split the tree up into subtrees with 7 and 35 marked points. Then Jac $\mathcal{X}_{61}$ has bad reduction, and thus does not have CM.

The program `stable_reduction.sage` gives the tree $\Gamma_{\overline{\mathcal{Y}}}$ for reduction modulo 2.

- For $\mathcal{X}_{21}$, there is an edge splitting $\Gamma_{\overline{\mathcal{Y}}}$ into two trees with 6 and 12 markings, and $n = 3$.
- For $\mathcal{X}_{42}$, there is an edge splitting $\Gamma_{\overline{\mathcal{Y}}}$ into two trees with 6 and 24 markings, and $n = 3$.
- For $\mathcal{X}_{54}$, there is an edge splitting $\Gamma_{\overline{\mathcal{Y}}}$ into two trees with 10 and 40 markings, and $n = 5$.
- For $\mathcal{X}_{59}$, there is an edge splitting $\Gamma_{\overline{\mathcal{Y}}}$ into two trees with 6 and 36 markings, and $n = 3$.

In all cases $i \in \{21, 42, 54, 59\}$, using Prop. as before one shows that $\Gamma_{\overline{\mathcal{X}_i}}$ is not a tree, which means that Jac $\mathcal{X}$ has bad reduction, and thus does not have CM.

Cor. None of the curves $\mathcal{X}_{22}$, $\mathcal{X}_{23}$, $\mathcal{X}_{24}$, $\mathcal{X}_{44}$, $\mathcal{X}_{46}$, $\mathcal{X}_{47}$, $\mathcal{X}_{56}$, or $\mathcal{X}_{63}$ in Table 1 has CM Jacobian.

Frobenius criterion, I

Let A be an abelian variety defined over a number field K. For any prime $\mathfrak{p}$ of K where A has good reduction, let $f_\mathfrak{p} \in \mathbb{Q}[T]$ be the minimal polynomial of the Frobenius at $\mathfrak{p}$ acting on the Tate module of the reduction of A modulo $\mathfrak{p}$.

Let $E_{f_\mathfrak{p}}$ equal $\mathbb{Q}[T]/f_\mathfrak{p}$. Since the Frobenius action is semisimple, the polynomial $f_\mathfrak{p}$ has no multiple factors.

If t is the image of T in $E_{f_\mathfrak{p}}$, then let $E'_{f_\mathfrak{p}} \subseteq E_{f_\mathfrak{p}}$ be the subring given by intersecting the rings of $\mathbb{Q}[t^n]_{n \in \mathbb{N}}$ inside $E_{f_\mathfrak{p}}$. Observe that, if $f_\mathfrak{p} = g(T^m)$ for some polynomial g and $m \in \mathbb{N}$, we can replace $f_\mathfrak{p}$ by $g(T)$ when computing $E'_{f_\mathfrak{p}}$.

The following criterion can be used to show that A does not have CM.
Prop:If $\dim(A) = g$ and A has CM, then there exists a product of number fields E with $\dim_\mathbb{Q} E \leq 2g$ such that for any good prime $\mathfrak{p}$, we have an embedding $E'_{f_\mathfrak{p}} \hookrightarrow E$.

Before our main application we prove two lemmas.

Lemma: If $K_1, \ldots, K_n$ and $L_1, \ldots, L_m$, are characteristic 0 fields, then there exists a $\mathbb{Q}$-algebra embedding of $K_1 \times \cdots \times K_n$ into $L_1 \times \cdots \times L_m$ if and only if there exists a surjective map $\phi : \{1, \ldots, m\} \to \{1, \ldots, n\}$ such that for all $i \in \{1, \ldots, m\}$, there exists an embedding $\gamma_i : K_{\phi(i)} \hookrightarrow L_i$.

Frobenius criterion, II

Lemma: The curves $\mathcal{X}_5$, $\mathcal{X}_6$, $\mathcal{X}_{26}$, $\mathcal{X}_{29}$, $\mathcal{X}_{33}$, $\mathcal{X}_{43}$, and $\mathcal{X}_{66}$ from Table 1 have quotients with the following affine equations, respectively, where i is a square root of -1:

Curve	Affine Birational Equation of Quotient Curve
$\mathcal{X}_5$	$y^3 = x^6 - 33x^4 - 33x^2 + 1$
$\mathcal{X}_6$	$y^4 = x^6 - 33x^4 - 33x^2 + 1$
$\mathcal{X}_{26}$	$y^7 = (x^4 - 4ix^2 + 12)(x^2 - 2i)$
$\mathcal{X}_{29}$	$y^{13} = (x^2 - 4)^7(x + 14)(x - 34)$
$\mathcal{X}_{33}$	$y^5 = x^{10} + 10x^8 + 35x^6 - 228x^5 + 50x^4 - 1140x^3 + 25x^2 - 1140x + 496$
$\mathcal{X}_{43}$	$y^5 = x^6 + 522x^5 - 10005x^4 - 10005x^2 - 522x + 1$
$\mathcal{X}_{66}$	$y^{31} = (x^2 - 228x + 496)^2(x^2 + 522x - 10004)^2(x + 11)^2(x^2 + 4)$

For each curve, we use the the program `frobenius_polynomials.sage` to compute the algebras $E'_{f,\mathfrak{p}}$ for various p, and then we show that it is impossible for all the $E'_{f,\mathfrak{p}}$ to embed into a $\mathbb{Q}$-algebra of the correct dimension.

Prop: None of the curves $\mathcal{X}_2$, $\mathcal{X}_5$, $\mathcal{X}_6$, $\mathcal{X}_{26}$, $\mathcal{X}_{29}$, $\mathcal{X}_{33}$, $\mathcal{X}_{43}$, or $\mathcal{X}_{66}$in Table 1 has CM Jacobian.

Cor: None of the curves $\mathcal{X}_3$, $\mathcal{X}_7$, $\mathcal{X}_8$, or $\mathcal{X}_{45}$ in Table 1 has CM Jacobian.

Summarizing

Now we are ready to state the main theorem. Recall that if $\mathcal{X}$ is a smooth superelliptic curve with reduced automorphism group A_4, S_4, and A_5, then $\mathcal{X}$ is given in Table 1.

Theorem

For each case whether or not Jac $\mathcal{X}$ has CM is determined in the 6th column.

Corollary

For superelliptic curves with many automorphisms, having complex multiplication is equivalent to satisfying Streit's Criterion.

Where do we go from here?

- Can we extend these results to positive characteristic? Would they have any significance in cryptography?
- Can we extend these results to generalized superelliptic curves?
- What about other curves with many automorphism? There are non-superelliptic curves with many automorphisms. Are they CM type?
- Is the following statement true?
  If $\mathcal{X}$ is a CM curve, then $\mathcal{X}$ is defined over the field of moduli.
- It is believed that for$\mathcal{X}$ having lots of automorphisms places upward pressure on the End ^{0}(Jac $\mathcal{X}$). An interesting family of curves would be curves with large automorphism groups as determined in (Magaard et al., 2002).
- It would also be interesting to obtain a theoretical explanation for Cor. 1.
- Can CM points in $\mathcal{M}_g$ be classified in terms of the GIT height?

References, I

Bouw, Irene I. and Stefan Wewers. 2017. *Computing L-functions and semistable reduction of superelliptic curves*, Glasg. Math. J. **59**, no. 1, 77–108. MR3576328

Deuring, Max. 1941. *Die Typen der Multiplikatorenringe elliptischer Funktionenkörper*, Abh. Math. Sem. Hansischen Univ. **14**, 197–272. MR5125

______. 1949. *Algebraische Begründung der komplexen Multiplikation*, Abh. Math. Sem. Univ. Hamburg **16**, no. nos., nos. 1-2, 32–47. MR32601

Frediani, Paola, Alessandro Ghigi, and Matteo Penegini. 2015. *Shimura varieties in the Torelli locus via Galois coverings*, Int. Math. Res. Not. IMRN **20**, 10595–10623. MR3455876

Hidalgo, Ruben A., Saul Quispe, and Tony Shaska. 2016. *On generalized superelliptic Riemann surfaces*, arxiv:1609.09576.

Magaard, K., T. Shaska, S. Shpectorov, and H. Völklein. 2002. *The locus of curves with prescribed automorphism group*, Sūrikaisekikenkyūsho Kōkyūroku **1267**, 112–141. Communications in arithmetic fundamental groups (Kyoto, 1999/2001). MR1954371

Mueller, Nicolas. 2017. *Hyperelliptic curves with many automorphisms.* Masters Thesis, available at https://people.math.ethz.ch/∼pink/Theses/2017-Master-Nicolas-Mueller.pdf.

Müller, Nicolas and Richard Pink. 2017. *Hyperelliptic curves with many automorphisms*, arXiv:1711.06599.

Mumford, David. 2008. *Abelian varieties*, Tata Institute of Fundamental Research Studies in Mathematics, vol. 5, Published for the Tata Institute of Fundamental Research, Bombay; by Hindustan Book Agency, New Delhi. With appendices by C. P. Ramanujam and Yuri Manin, Corrected reprint of the second (1974) edition. MR2514037

Obus, Andrew and Tanush Shaska. 2021. *Superelliptic curves with many automorphisms and CM Jacobians*, Math. Comp. **90**, no. 332, 2951–2975. MR4305376

Oort, Frans. 1988. *Endomorphism algebras of abelian varieties*, Algebraic geometry and commutative algebra, Vol. II, pp. 469–502. MR977774

Sanjeewa, R. and T. Shaska. 2008. *Determining equations of families of cyclic curves.*, Albanian J. Math. **2**, no. 3, 199–213 (English).

Schmidt, Claus-Günther. 1984. *Arithmetik abelscher Varietäten mit komplexer Multiplikation*, Lecture Notes in Mathematics, vol. 1082, Springer-Verlag, Berlin. With an English summary. MR822472

References, II

Shaska, T. and H. Völklein. 2004. *Elliptic subfields and automorphisms of genus 2 function fields*, Algebra, arithmetic and geometry with applications (West Lafayette, IN, 2000), pp. 703–723. MR2037120 (2004m:14047)

Shimura, Goro and Yutaka Taniyama. 1961. *Complex multiplication of abelian varieties and its applications to number theory*, Publications of the Mathematical Society of Japan, vol. 6, The Mathematical Society of Japan, Tokyo. MR0125113

Streit, M. 2001. *Period matrices and representation theory*, Abh. Math. Sem. Univ. Hamburg **71**, 279–290. MR1873049

Team, The Sage Development. 2020. *Sage mathematics software*, Sagemath.

Towse, Christopher. 1996. *Weierstrass points on cyclic covers of the projective line.*, Trans. Amer. Math. Soc. **348**, no. 8, 3355–3378.

Thank you for your attention!