Mathematics
Research
Reports

Yuri Zarhin

Jacobians with automorphisms of prime order

Volume 7 (2026), p. 1-26.

https://doi.org/10.5802/mrr.24

CENTRE MERSENNE

Mathematics Research Reports *is member of the Centre Mersenne for Open Scientific Publishing*
www.centre-mersenne.org
e-ISSN: 2772-9559

Mathematics Research Reports
Volume 7 (2026), 1–26

Jacobians with automorphisms of prime order

Yuri Zarhin

(Recommended by Boris Hasselblatt)

Dedicated to Frans Oort on the occasion of his 90th birthday

Abstract. In this paper we study principally polarized complex abelian varieties (X,λ) that admit an automorphism δ of prime order $p>2$. It turns out that certain natural conditions on the multiplicities of the action of δ on $\Omega^1(X)$ do guarantee that those polarized varieties are not canonically polarized jacobians of curves.

1. Introduction

The work of Clemens and Griffiths [5] on intermediate jacobians of threefolds and their applications to the Lüroth problem increased an interest in the classical question—how to find out that a given principally polarized g-dimensional complex abelian variety (X,λ) is not isomorphic to the canonically polarized jacobian $(\mathcal{J},\Theta)$ of a smooth irreducible projective curve $\mathcal{C}$ of genus g. In this paper we address this question in the case when (X,λ) admits an additional symmetry—an automorphism δ of prime period $p>2$ that satisfies the pth cyclotomic equation. Choosing once and for all a primitive pth root of unity ζ_p, we give our answer in terms of the *multiplicity function* $\mathbf{a}_{X,\delta}$, which assigns to each $h\in(\mathbb{Z}/p\mathbb{Z})^*$ the multiplicity $\mathbf{a}_X(h)$ of the eigenvalue ζ_p^h of the linear operator δ_Ω in the space $\Omega^1(X)$ of differentials of the first kind on X induced by δ.

Namely, we describe explicitly all integer-valued (we call them *strongly admissible*) functions $f:(\mathbb{Z}/p\mathbb{Z})^*\to\mathbb{Z}_+$ that enjoy the following property: there exists a triple $(\mathcal{J},\Theta,\delta)$ as above such that $f=\mathbf{a}_{\mathcal{J},\delta}$.

It turns out that not every function $\mathbf{a}_{X,\delta}$ coincides with some $\mathbf{a}_{\mathcal{J},\delta}$. For example, if $p=3$ then there are precisely $(g+1)$ functions of type $\mathbf{a}_{X,\delta}$; however, there are approximately only $g/3$ functions of type $\mathbf{a}_{\mathcal{J},\delta}$ (Section 4, see also [21]).

The paper is organized as follows. In Section 2 we study canonically polarized jacobians $(\mathcal{J},\Theta)$ of curves $\mathcal{C}$ such that there is automorphism $\delta\in\mathrm{Aut}(\mathcal{J},\Theta)$ with properties described above. It turns out that δ is induced by an automorphism $\delta_{\mathcal{C}}$ of $\mathcal{C}$ of order p. It turns out that the number of fixed points of $\delta_{\mathcal{C}}$ is $\frac{2g}{p-1}+2$ and each of these points P is nondegenerate, i.e., its *index* ϵ_P is a primitive pth root of unity. This gives rise to the integer-valued function $\mathbf{b}:(\mathbb{Z}/p\mathbb{Z})^*\to\mathbb{Z}_+$ that assigns to each $h\in(\mathbb{Z}/p\mathbb{Z})^*$ the number of fixed points of $\delta_{\mathcal{C}}$ with index ζ_p^h. Our main result (Theorem 2.1) expresses explicitly the function $\mathbf{a}_{\mathcal{J},\delta}$ in terms of the function $\mathbf{b}$, which imposes restrictions on the function $\mathbf{a}_{\mathcal{J},\delta}$. In Section 3 we prove Theorem 3.1, which implies that the necessary condition for a function $f:(\mathbb{Z}/p\mathbb{Z})^*\to\mathbb{Z}_+$ to coincide with some $\mathbf{a}_{\mathcal{J},\delta}$ imposed by Theorem 3.1 is actually sufficient. In Section 4 we discuss in detail the case $p=3$. Section 5 deals with

Received January 31, 2025; revised November 18, 2025.
2020 *Mathematics Subject Classification.* 14J45, 14K30.
Keywords. Jacobians, polarizations, endomorphisms rings of abelian varieties.

CM abelian varieties of dimension $(p-1)/2$. In Section 6 we discuss certain principally polarized abelian varieties that are not isomorphic as an algebraic variety to jacobians.

2. Principally polarized abelian varieties with automorphisms

We write $\mathbb{Z}_+$ for the set of *nonnegative* integers, $\mathbb{Q}$ for the field of rational numbers and $\mathbb{C}$ for the field of complex numbers. We have

$$\mathbb{Z}_+ \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C},$$

where $\mathbb{Z}$ is the ring of integers and $\mathbb{R}$ is the field of real numbers. If B is a finite (may be, empty) set then we write $\#(B)$ for its cardinality. Let p be an odd prime and $\zeta_p \in \mathbb{C}$ a primitive (complex) pth root of unity. It generates the multiplicative order p cyclic group μ_p of pth roots of unity. We write $\mathbb{Z}[\zeta_p]$ and $\mathbb{Q}(\zeta_p)$ for the pth cyclotomic ring and the pth cyclotomic field respectively. We have

$$\zeta_p \in \mu_p \subset \mathbb{Z}[\zeta_p] \subset \mathbb{Q}(\zeta_p) \subset \mathbb{C}.$$

Let $g \ge 1$ be an integer and (X, λ) a principally polarized g-dimensional abelian variety over $\mathbb{C}$, δ an automorphism of (X, λ) that satisfies the cyclotomic equation

$$\sum_{j=0}^{p-1} \delta^j = 0 \in \mathrm{End}(X). \tag{2.1}$$

In other words, δ is a periodic automorphism of order p, whose set of fixed points is finite. This gives rise to the embeddings

$$\mathbb{Z}[\zeta_p] \hookrightarrow \mathrm{End}(X), \qquad 1 \mapsto 1_X, \quad \zeta_p \mapsto \delta;$$
$$\mathbb{Q}(\zeta_p) \hookrightarrow \mathrm{End}(X) \otimes \mathbb{Q} =: \mathrm{End}^0(X), \quad 1 \mapsto 1_X, \quad \zeta_p \mapsto \delta.$$

(Hereafter we write 1_X for the identity automorphism of X.) Since the degree $[\mathbb{Q}(\zeta_p) : \mathbb{Q}] = p-1$, it follows from [17, Ch. 2, Prop. 2] (see also [16, Part II, p. 767]) that

$$(p-1) \mid 2g. \tag{2.2}$$

By functoriality, $\mathbb{Q}(\zeta_p)$ acts on the g-dimensional complex vector space $\Omega^1(X)$ of differentials of the first kind on X. This endows $\Omega^1(X)$ with the structure of a $\mathbb{Q}(\zeta_p) \otimes_{\mathbb{Q}} \mathbb{C}$-module. Clearly,

$$\mathbb{Q}(\zeta_p) \otimes_{\mathbb{Q}} \mathbb{C} = \oplus_{j=1}^{p-1} \mathbb{C}$$

where the jth summand corresponds to the field embedding $\mathbb{Q}(\zeta_p) \hookrightarrow \mathbb{C}$ that sends ζ_p to ζ_p^j. So, $\mathbb{Q}(\zeta_p)$ acts on $\Omega^1(X)$ with multiplicities a_j $(j = 1, \dots p-1)$. Clearly, all a_j are nonnegative integers and

$$\sum_{j=1}^{p-1} a_j = g. \tag{2.3}$$

In addition,

$$a_j + a_{p-j} = \frac{2g}{p-1} \ \forall j = 1, \dots p-1; \tag{2.4}$$

this is a special case of a general well known result about endomorphism fields of complex abelian varieties: see, e.g., [12, p. 84]. (See also Remark 2 below where another proof for jacobians is given.) We may view the collection $\{a_j\}$ as a nonnegative integer-valued function

$$\mathbf{a} = \mathbf{a}_{X,\delta}$$

on the finite cyclic group $G = (\mathbb{Z}/p\mathbb{Z})^*$ of order $(p-1)$ where

$$\mathbf{a}_{X,\delta}(j \bmod p) = \mathbf{a}(j \bmod p) = a_j \ (1 \le j \le p-1); \quad \sum_{h \in G} \mathbf{a}_{X,\delta}(h) = g. \tag{2.5}$$

The group G contains two distinguished elements, namely, the identity element 1 mod p and the only element (-1) mod $p = (p-1)$ mod p of order 2. If h is an element of G then we write $-h$ for the product of h by (-1) mod p in G. If $h = j$ mod p then $-h = (p-j)$ mod p. In light of (2.4),

$$\mathbf{a}_{X,\delta}(h) + \mathbf{a}_{X,\delta}(-h) = \frac{2g}{p-1} \ \forall h \in G. \tag{2.6}$$

For each $h = j$ mod $p \in G$ we write

$$\zeta_p^h := \zeta_p^j,$$

which is a primitive pth root of unity that does *not* depend on the choice of j.

Definition 1. *Let p be an odd prime and g a positive integer such that $p-1$ divides $2g$. Let $f: G \to \mathbb{Z}_+$ be a nonnegative integer-valued function.*

(i) *We say that f is* well rounded *of degree g if*

$$f(h) + f(-h) = \frac{2g}{p-1} \ \forall h \in G.$$

(ii) *We say that f is* admissible *of degree g if there exist a principally polarized g-dimensional complex abelian variety (X,λ) with an automorphism $\delta \in \mathrm{Aut}(X,\lambda)$ of period p such that* (2.1) *holds and*

$$f = \mathbf{a}_{X,\delta}.$$

(iii) *We say that f is* strongly admissible *of degree g if it is admissible of degree g and one may choose the corresponding (X,λ,δ) in such a way that (X,λ) is the canonically polarized jacobian of a smooth irreducible connected projective curve of genus g.*

Remark 1.

(i) *In light of* (2.6), *our $\mathbf{a} = \mathbf{a}_{X,\delta}$ is well rounded. In other words, every admissible function is well rounded.*

(ii) *The number of well rounded functions (for given g and p) is obviously*

$$\left(\frac{2g}{p-1}+1\right)^{(p-1)/2}.$$

(iii) *Let $f: G \to \mathbb{Z}_+$ be a well rounded function of degree g. Then*

$$\bar{f}: G \to \mathbb{Z}_+,\ h \mapsto f(-h) = \frac{2g}{p-1} - f(h)$$

is also well rounded of degree g. In addition, if f is admissible (resp. strongly admissible) then $\bar{f}$ is also admissible (resp. strongly admissible). Namely, let (X,λ) be a principally polarized abelian variety, $\delta \in \mathrm{Aut}(X,\lambda)$ an automorphism of period p that satisfies the pth cyclotomic equation (2.1) *in* $\mathrm{End}(X)$ *and such that f coincides with the corresponding multiplicity function $\mathbf{a}_{X,\delta}$. Then δ^{-1} is also an automorphism of* $\mathrm{Aut}(X,\lambda)$ *of period p that satisfies the pth cyclotomic equation and such that $\bar{f} = \mathbf{a}_{X,\delta^{-1}}$. So, $\bar{f}$ is admissible. In addition, if $(X,\lambda) = (\mathcal{J}(\mathcal{C}),\Theta)$ is the canonically polarized jacobian of a curve $\mathcal{C}$ then $\bar{f} = \mathbf{a}_{\mathcal{J}(\mathcal{C}),\delta^{-1}}$ is strongly admissible.*

Example 1. *Let $p = 3$ and E an elliptic curve over $\mathbb{C}$ with complex multiplication by $\mathbb{Z}[\zeta_3]$. We may take as E the smooth projective model of $y^2 = x^3 - 1$ where ζ_3 acts on E by an automorphism*

$$\delta_E : (x,y) \mapsto (\zeta_3 x, y).$$

Clearly, δ_E *satisfies the 3rd cyclotomic equation and respects the only principal polarization on* E*. We have*

$$\Omega^1(E) = \mathbb{C}\cdot\frac{dx}{y}, \quad (\delta_E)_\Omega\left(\frac{dx}{y}\right) = \frac{d(\zeta_3 x)}{y} = \zeta_3\frac{dx}{y}.$$

This means that

$$\mathbf{a}_{E,\delta_E}(1 \bmod 3) = 1, \quad \mathbf{a}_{E,\delta_E}(2 \bmod 3) = 0.$$

Let g *be a positive integer, and let* $f(1)$ *and* $f(2)$ *be nonnegative integers, whose sum is* g*. Let us put*

$$Y_1 = E^{f(1)}, \quad Y_2 = E^{f(2)}, \quad Y = Y_1 \times Y_2.$$

Let λ_Y *be the principal polarization on* Y *that is the product of* g *pull-backs of the principal polarization on* E*. Let us consider the automorphism* δ_Y *of* Y *that acts (diagonally) as* δ_E *on* $Y_1 = E^{f(1)}$ *and as* $\delta_E^2 = \delta_E^{-1}$ *on* $Y_2 = E^{f(2)}$*. Clearly,* δ_Y *satisfies the 3rd cyclotomic equation and respects* λ_Y*. It is also clear that*

$$\mathbf{a}_{Y,\delta_Y}(1 \bmod 3) = f(1), \quad \mathbf{a}_{Y,\delta_Y}(2 \bmod 3) = f(2).$$

In other words, if $p = 3$ *then every well rounded function of degree* g *is admissible. We will see (Section 4 below) that not every such function is strongly admissible.*

We will also need the function

$$\mathbf{j}: G = (\mathbb{Z}/p\mathbb{Z})^* \to \mathbb{Z}, \ (j \bmod p) \mapsto j \ (1 \le j \le p-1). \tag{2.7}$$

Clearly,

$$\mathbf{j}(h_1 h_2) \equiv \mathbf{j}(h_1)\mathbf{j}(h_2) \bmod p \ \forall h_1, h_2 \in G. \tag{2.8}$$

Recall that if $f_1(h)$ and $f_2(h)$ are complex-valued functions on G then their convolution is the function $f_1 * f_2(h)$ on G defined by

$$f_1 * f_2(h) = \frac{1}{p-1}\sum_{u\in G} f_1(u) f_2(u^{-1}h). \tag{2.9}$$

Theorem 2.1. *Suppose that* (X,λ) *is the jacobian of a smooth projective irreducible genus* g *curve* $\mathcal{C}$ *with canonical principal polarization. Then there exists a nonnegative integer-valued function*

$$\mathbf{b}: G = (\mathbb{Z}/p\mathbb{Z})^* \to \mathbb{Z}_+ \subset \mathbb{C}$$

such that

$$\sum_{h\in G}\mathbf{b}(h) = \frac{2g}{p-1} + 2, \quad \sum_{h\in G}\mathbf{b}(h)\mathbf{j}(h^{-1}) \in p\mathbb{Z}, \tag{2.10}$$

$$\mathbf{a}(v) := \mathbf{a}_{X,\delta}(v) = \frac{(p-1)}{p}\cdot\mathbf{b} * \mathbf{j}(-v) - 1 \ \forall v \in G. \tag{2.11}$$

Example 2. *Let us describe explicitly the case* $g = 1$*. Then* X *is an elliptic curve. It follows from* (2.2) *that* $(p-1)$ *divides* 2 *and therefore*

$$p = 3, \ p-1 = 2, \ G = (\mathbb{Z}/3\mathbb{Z})^* = \{\bar{1} = 1 \bmod 3, \ \bar{2} = 2 \bmod 3 = -\bar{1}\}.$$

Then either

$$\mathbf{a}_{X,\delta}(\bar{1}) = 1, \quad \mathbf{a}_{X,\delta}(\bar{2}) = 0 \tag{2.12}$$

or

$$\mathbf{a}_{X,\delta}(\bar{1}) = 0, \quad \mathbf{a}_{X,\delta}(\bar{2}) = 1. \tag{2.13}$$

In the case (2.12)*, the desired* $\mathbf{b}$ *is given by the formulas*

$$\mathbf{b}(\bar{1}) = 0, \quad \mathbf{b}(\bar{2}) = 3.$$

In the case (2.13)*, the desired* **b** *is given by the formulas*

$$\mathbf{b}(\bar{1}) = 3, \quad \mathbf{b}(\bar{2}) = 0.$$

Proof of Theorem 2.1. In light of Example 2, we may assume that $g > 1$. We may assume that $(X, \lambda) = (\mathcal{J}(\mathcal{C}), \Theta)$ where $\mathcal{C}$ is an irreducible smooth projective genus g curve, $\mathcal{J}(\mathcal{C})$ is its jacobian with canonical principal polarization Θ, and

$$\delta \in \mathrm{Aut}(\mathcal{J}(\mathcal{C}), \Theta)$$

satisfies the pth cyclotomic equation

$$\sum_{i=0}^{p-1} \delta^i = 0 \in \mathrm{End}(\mathcal{J}(\mathcal{C})).$$

This means that $\delta^p = 1 \in \mathrm{End}(\mathcal{J}(\mathcal{C}))$ and the (sub)set $\mathcal{J}(\mathcal{C})^{\delta}$ of δ-invariant points of $\mathcal{J}$ is finite. The latter implies that the homomorphism $1_{\mathcal{J}(\mathcal{C})} - \delta : \mathcal{J}(\mathcal{C}) \to \mathcal{J}(\mathcal{C})$ has finite kernel, hence, is *surjective*.

Identifying the curve $\mathcal{C}$ with its image $\mathrm{alb}_{P_0}(\mathcal{C}) \subset \mathcal{J}(\mathcal{C})$ (i.e., $\mathrm{alb}(P_0)$ is the zero 0 of the group law on $\mathcal{J}(\mathcal{C})$), we have

$$0 = \mathrm{alb}_{P_0}(P_0) \in \mathcal{C} \subset \mathcal{J}(\mathcal{C}).$$

If $v \in X = \mathcal{J}(\mathcal{C})$ then we write T_v for the translation map

$$T_v : X \to X, \quad x \mapsto x + v.$$

By Torelli Theorem (Weil's variant, see [18, p. 35, Hauptsatz] and [19]) applied to

$$\delta^{(p+1)/2} \in \mathrm{Aut}(\mathcal{J}(\mathcal{C}), \Theta),$$

$\exists\, \phi_{1/2} \in \mathrm{Aut}(\mathcal{C})$, $\epsilon = \pm 1$, and $z \in \mathcal{J}(\mathcal{C})$ such that

$$\delta^{(p+1)/2}(P) = \epsilon\, \phi_{1/2}(P) + z \ \ \forall P \in \mathcal{C} \subset \mathcal{J}(\mathcal{C}).$$

This implies that

$$\begin{aligned}
\delta(P) = \delta^{p+1}(P) &= \left(\delta^{(p+1)/2}\right)^2(P) = \delta^{(p+1)/2}\left(\epsilon\, \phi_{1/2}(P) + z\right) \\
&= \epsilon\, \delta^{(p+1)/2}\left(\phi_{1/2}(P)\right) + \delta^{(p+1)/2}(z) = \epsilon\left(\epsilon \phi_{1/2}^2(P) + z\right) + \delta^{(p+1)/2}(z) \\
&= \epsilon^2 \phi_{1/2}^2(P) + \left(\epsilon\, z + \epsilon \delta^{(p+1)/2} z\right) = \phi_{1/2}^2(P) + \left(\epsilon\, z + \epsilon \delta^{(p+1)/2} z\right).
\end{aligned}$$

It follows that $\delta(P) = \phi_{1/2}^2(P) - w$ with $w = -(\epsilon\, z + \epsilon\, \delta^{(p+1)/2} z)$. Let us put

$$\phi := \phi_{1/2}^2 \in \mathrm{Aut}(\mathcal{C}).$$

Then

$$\phi(P) = \delta(P) + w = T_w \circ \delta(P) \quad \forall P \in \mathcal{C} \subset \mathcal{J}(\mathcal{C}), \tag{2.14}$$

i.e., the following diagram is commutative. (Here the horizontal arrows are the inclusion map alb_{P_0}.)

$$\begin{array}{ccc}
\mathcal{C} & \xrightarrow{\subset} & \mathcal{J}(\mathcal{C}) \\
\phi \downarrow & & \downarrow T_w \circ \delta \\
\mathcal{C} & \xrightarrow{\subset} & \mathcal{J}(\mathcal{C})
\end{array}$$

Choose $v \in \mathcal{J}(\mathcal{C})$ such that $v - \delta(v) = (1 - \delta)v = w$. Then

$$T_w \circ \delta = T_v \circ \delta \circ T_v^{-1},$$

i.e., $T_w \circ \delta$ and δ are conjugate in the group $\tilde{\mathrm{Aut}}(\mathcal{J}(\mathcal{C}))$ of biregular automorphisms of the *algebraic variety* $\mathcal{J}(\mathcal{C})$. In particular, $T_w \circ \delta$ is a periodic automorphism of order p;

hence, ϕ^p is the *identity automorphism* of $\mathscr{C}$. On the other hand, ϕ itself is *not* the identity map (see below).

It is well known that the map $\Psi : \Omega^1(\mathscr{J}(\mathscr{C})) \to \Omega^1(\mathscr{C})$ induced by the inclusion map $\mathrm{alb}_{P_0} : \mathscr{C} \subset \mathscr{J}(\mathscr{C})$ is an isomorphism of g-dimensional complex vector spaces. On the other hand, the linear map $(T_u)_\Omega : \Omega^1(\mathscr{J}(\mathscr{C})) \to \Omega^1(\mathscr{J}(\mathscr{C}))$ induced by any translation $T_u : \mathscr{J}(\mathscr{C})) \to \mathscr{J}(\mathscr{C}))$ is the *identity map* for all u (because all global regular 1-forms on an abelian variety are translation-invariant). Hence, the linear maps $\delta_\Omega : \Omega^1(\mathscr{J}(\mathscr{C})) \to \Omega^1(\mathscr{J}(\mathscr{C}))$ and $(T_w \circ \delta)_\Omega : \Omega^1(\mathscr{J}(\mathscr{C})) \to \Omega^1(\mathscr{J}(\mathscr{C}))$ induced by δ and $T_w \circ \delta$ respectively do coincide. This implies that the following diagram is commutative.

$$\begin{array}{ccc} \Omega^1(\mathscr{J}(\mathscr{C})) & \xrightarrow{\Psi} & \Omega^1(\mathscr{C}) \\ {\scriptstyle \delta_\Omega=(T_w\circ\delta)_\Omega}\big\downarrow & & \big\downarrow{\scriptstyle \phi_\Omega} \\ \Omega^1(\mathscr{J}(\mathscr{C})) & \xrightarrow{\Psi} & \Omega^1(\mathscr{C}) \end{array}.$$

It follows that

$$\phi_\Omega = \Psi \circ \delta_\Omega \circ \Psi^{-1}.$$

In particular, the linear operators ϕ_Ω and δ_Ω have the the same spectrum, the same trace, and ϕ_Ω is an automorphism of order p. This implies that ϕ is *not* the identity map, hence, has order p. The action of ϕ on $\mathscr{C}$ gives rise to the group embedding

$$\mu_p \hookrightarrow \mathrm{Aut}(\mathscr{C}), \quad \zeta_p \mapsto \phi.$$

Let $P \in \mathscr{C}$ be a fixed point of ϕ. Then ϕ induces an automorphism of the corresponding (one-dimensional) tangent space $\mathscr{T}_P(\mathscr{C})$ that is multiplication by a complex number ϵ_P that is called the *index* of P. Clearly, ϵ_P is a pth root of unity.

Lemma 1. *Every fixed point P of ϕ is nondegenerate, i.e., $\epsilon_P \ne 1$.*

Proof of Lemma 1. The result is well-known. but I failed to find a proper reference (however, see [21, Lemma 1.2]) where the case $p = 3$ was proven.)

Suppose that $\epsilon_P = 1$. Let $\mathscr{O}_P$ be the local ring of $\mathscr{C}$ at P and $\mathfrak{m}_P$ its maximal ideal. We write ϕ_* for the automorphism of $\mathscr{O}_P$ induced by ϕ. Clearly, ϕ_*^p is the identity map. Since ϕ is *not* the identity map, there are no ϕ_*-invariant local parameters at P. Clearly, $\phi_*(\mathfrak{m}_P) = \mathfrak{m}_P, \phi_*(\mathfrak{m}_P^2) = \mathfrak{m}_P^2$. Since $\mathscr{T}_P(\mathscr{C})$ is the dual of $\mathfrak{m}_P/\mathfrak{m}_P^2$ and $\epsilon_p = 1$, we conclude that ϕ_* induces the identity map on $\mathfrak{m}_P/\mathfrak{m}_P^2$. This implies that if $t \in \mathfrak{m}_P$ is a local parameter at P (i.e., its image $\bar{t}$ in $\mathfrak{m}_P/\mathfrak{m}_P^2$ is *not* zero) then

$$t' := \sum_{k=0}^{p-1} \phi_*^k(t) \in \mathfrak{m}_P \subset \mathscr{O}_P$$

is ϕ_*-invariant and its image in $\mathfrak{m}_P/\mathfrak{m}_P^2$ equals $p\bar{t} \ne 0$. This implies that t' is a ϕ_*-invariant local parameter at P. Contradiction. □

Corollary 1. *The quotient $\mathscr{D} := \mathscr{C}/\mu_p$ is a smooth projective irreducible curve. The map $\mathscr{C} \to D$ has degree p, its ramification points are exactly the fixed points of ϕ and all the ramification indices are p.*

Lemma 2. *$\mathscr{D}$ is biregularly isomorphic to the projective line.*

Proof of Lemma 2. Suppose that the genus of $\mathscr{D}$ is positive. Then there is a nonzero $\omega_0 \in \Omega^1(\mathscr{D})$. Its inverse image ω in $\Omega^1(\mathscr{C})$ is a nonzero ϕ_Ω-invariant regular 1-form. Hence, the spectrum of ϕ_Ω contains 1. We have seen that the linear operators ϕ_Ω and δ_Ω have the same spectrum. Hence, the spectrum of δ_Ω contains 1, which is not the case. The obtained contradiction proves that the genus of $\mathscr{D}$ is 0. □

Corollary 2. *The number $F(\phi)$ of fixed points of ϕ is $\frac{2g}{p-1}+2$.*

Proof of Corollary 2. Applying the Riemann-Hurwitz formula to $\mathscr{C}\to\mathscr{D}$, we get

$$2g-2=p\cdot(-2)+(p-1)\cdot F(\phi). \qquad \square$$

Lemma 3. *Let τ be the trace of $\phi_\Omega:\Omega^1(\mathscr{C})\to\Omega^1(\mathscr{C})$. Then*

$$\tau=\sum_{j=1}^{p-1}a_j\zeta_p^j=\sum_{h\in G}\mathbf{a}(h)\zeta_p^h.$$

Proof of Lemma 3. We have seen that the linear operators ϕ_Ω and δ_Ω have the same trace. Now the very definition of a_j's implies that the trace of δ_Ω equals $\sum_{j=1}^{p-1}a_j\zeta_p^j$. Hence, $\tau=\sum_{j=1}^{p-1}a_j\zeta_p^j$. $\square$

Lemma 4. *Let $\zeta\in\mathbb{C}$ be a primitive pth root of unity. Then*

$$\frac{1}{1-\zeta}=-\frac{\sum_{j=1}^{p-1}j\zeta^j}{p}=-\frac{\sum_{h\in G}\mathbf{j}(h)\zeta^h}{p}. \tag{2.15}$$

Proof of Lemma 4. We have

$$(1-\zeta)\left(\sum_{j=1}^{p-1}j\zeta^j\right)=\sum_{j=1}^{p-1}\left(j\zeta^j-j\zeta^{j+1}\right)=\left(\sum_{j=1}^{p-1}\zeta^j\right)-(p-1)\zeta^p=(-1)-(p-1)=-p. \qquad \square$$

End of proof of Theorem 2.1. Let B be the set of fixed points of ϕ. We know that $\#(B)=\frac{2g}{p-1}+2$. By the holomorphic Lefschetz fixed point formula [3, Thm. 2], [6, Ch. 3, Sec. 4] (see also [10, Sec. 12.2 and 12.5]) applied to ϕ,

$$1-\bar{\tau}=\sum_{P\in B}\frac{1}{1-\epsilon_P} \tag{2.16}$$

where $\bar{\tau}$ is the complex-conjugate of τ. Recall that every ϵ_P is a primitive pth root of unity. Now Theorem 2.1 follows readily from the following assertion. $\square$

Proposition 2.2. *Let us define for each $h\in G$ the nonnegative integer $\mathbf{b}(h)$ as the number of fixed points $P\in B\subset\mathscr{C}(\mathbb{C})$ such that $\epsilon_P=\zeta_p^h$. Then*

$$\sum_{h\in G}\mathbf{b}(h)=F(\phi)=\frac{2g}{p-1}+2. \tag{2.17}$$

and

$$\mathbf{a}(v)=\frac{(p-1)}{p}\cdot\mathbf{b}*\mathbf{j}(-v)-1\ \forall v\in G. \tag{2.18}$$

In particular,

$$\mathbb{Z}\ni 1+\mathbf{a}(-1 \bmod p)=\frac{1}{p}\left(\sum_{h\in G}\mathbf{b}(h)\mathbf{j}(h^{-1})\right).$$

Proof of Proposition 2.2. The equality (2.17) is obvious. Let us prove (2.18). Combining (2.16) with Lemma 4 (applied to $\zeta=\zeta_p^h$) and Lemma 3, we get

$$\begin{aligned}1-\sum_{h\in G}\mathbf{a}(h)\zeta_p^{-h}&=\sum_{u\in G}\mathbf{b}(u)\frac{1}{1-\zeta_p^u}=\frac{-1}{p}\left(\sum_{u\in G}\mathbf{b}(u)\left(\sum_{h\in G}\mathbf{j}(h)\zeta_p^{hu}\right)\right)\\&=\frac{-1}{p}\sum_{v\in G}\left(\sum_{u\in G}\mathbf{b}(u)\mathbf{j}(u^{-1}v)\right)\zeta_p^v=\frac{-1}{p}\sum_{v\in G}(p-1)\mathbf{b}*\mathbf{j}(v)\zeta_p^v\\&=\frac{-(p-1)}{p}\sum_{v\in G}\mathbf{b}*\mathbf{j}(v)\zeta_p^v\end{aligned}$$

(here we use a substitution $v = hu$). Taking into account that

$$0 = 1 + \sum_{j=1}^{p-1} \zeta_p^j = 1 + \sum_{v \in G} \zeta_p^v,$$

we obtain

$$-\left(\sum_{v\in G} \zeta_p^v\right) - \sum_{h \in G} \mathbf{a}(h)\zeta_p^{-h} = -\frac{(p-1)}{p} \sum_{v\in G} \mathbf{b} * \mathbf{j}(v)\zeta_p^v.$$

Taking into account that the $(p-1)$-element set

$$\{\zeta_p^j \mid 1 \le j \le p-1\} = \{\zeta_p^v \mid v \in G\}$$

is a basis of the $\mathbb{Q}$-vector space $\mathbb{Q}(\zeta_p)$, we get $1 + \mathbf{a}(-v) = (p-1)\mathbf{b} * \mathbf{j}(v)/p$, i.e.,

$$\mathbf{a}(v) = \frac{(p-1)}{p} \cdot \mathbf{b} * \mathbf{j}(-v) - 1 \ \forall v \in G. \tag{2.19}$$

□

Remark 2. *Let us consider the function*

$$\mathbf{j}_0 := \mathbf{j} - \frac{p}{2} : G = (\mathbb{Z}/p\mathbb{Z})^* \to \mathbb{Q},\ (j \bmod p) \mapsto j - \frac{p}{2} \quad \textit{where } j = 1, \dots, p-1. \tag{2.20}$$

Then

$$\mathbf{j}_0(-u) = -\mathbf{j}_0(u) \ \forall u \in G. \tag{2.21}$$

If $\mathbf{a}, \mathbf{b} : G \to \mathbb{Z}_+$ *are functions related by* (2.19) *then*

$$\mathbf{b} * \mathbf{j}(v) = \mathbf{b} * \mathbf{j}_0(v) + \frac{p}{2(p-1)} \sum_{h\in G} \mathbf{b}(h) = \mathbf{b} * \mathbf{j}_0(v) + \frac{p}{2(p-1)}\left(\frac{2g}{p-1} + 2\right).$$

This implies that

$$\frac{(p-1)}{p} \cdot \mathbf{b} * \mathbf{j}(v) = \frac{(p-1)}{p} \cdot \mathbf{b} * \mathbf{j}_0(v) + \frac{g}{p-1} + 1$$

and therefore

$$\mathbf{a}(v) = \frac{(p-1)}{p} \cdot \mathbf{b} * \mathbf{j}_0(-v) + \frac{g}{p-1} \ \forall v \in G. \tag{2.22}$$

On the other hand, it follows from (2.21) *that the convolution* $\mathbf{b} * \mathbf{j}_0$ *also satisfies*

$$\mathbf{b} * \mathbf{j}_0(-v) = \mathbf{b} * \mathbf{j}_0(v) \ \ \forall v \in G.$$

This implies that

$$\mathbf{a}(v) + \mathbf{a}(-v) = \frac{(p-1)}{p} \cdot \mathbf{b} * \mathbf{j}_0(-v) + \frac{g}{p-1} + \frac{(p-1)}{p} \cdot \mathbf{b} * \mathbf{j}_0(v) + \frac{g}{p-1} = \frac{2g}{p-1} \ \forall v \in G.$$

This implies that

$$\mathbf{a}(v) + \mathbf{a}(-v) = \frac{2g}{p-1}. \tag{2.23}$$

(*Actually, we already know it for admissible* $\mathbf{a}$*, see* (2.4).) *It follows from* (2.23) *that*

$$\mathbf{a}(v) = \frac{2g}{p-1} - \frac{(p-1)}{p} \cdot \mathbf{b} * \mathbf{j}(v) + 1 \ \forall v \in G. \tag{2.24}$$

Corollary 3. *We keep the notation and assumptions of Theorem 2.1. Let* $\mathbf{b}' : G \to \mathbb{C}$ *be a complex-valued function on* g.

- (a) *The following two conditions are equivalent.*
  - (a1) $\mathbf{a}(v) = \frac{(p-1)}{p} \cdot \mathbf{b}' * \mathbf{j}(-v) - 1 \quad \forall v \in G.$

(a2) *The odd parts of functions* $\mathbf{b}$ *and* $\mathbf{b}'$ *coincide, i.e.,*

$$\mathbf{b}'(v)-\mathbf{b}'(-v)=\mathbf{b}(v)-\mathbf{b}(-v) \quad \forall v\in G; \tag{2.25}$$

in addition,

$$\sum_{h\in G}\mathbf{b}'(h)=\sum_{h\in G}\mathbf{b}(h)=\frac{2g}{p-1}+2. \tag{2.26}$$

(b) *If* $p=3$ *and condition (a1) holds then*

$$\mathbf{b}'(v)=\mathbf{b}(v)\ \forall v\in G.$$

Proof. If $f:G\to\mathbb{C}$ is a complex-valued function on g and $\chi:G\to\mathbb{C}^*$ is a character (group homomorphism) then we write

$$c_\chi(f)=\frac{1}{p-1}\sum_{h\in G}f(h)\bar{\chi}(h)$$

for the corresponding *Fourier coefficient* of f. For example, if $\chi_0\equiv 1$ is the *trivial character* of g then

$$c_{\chi_0}(f)=\frac{1}{p-1}\sum_{h\in G}f(h).$$

In particular,

$$c_{\chi_0}(\mathbf{j})=\frac{1}{p-1}\sum_{j=1}^{p-1}j=\frac{p}{2}\neq 0.$$

We have

$$f(v)=\sum_{\chi\in\hat{G}}c_\chi(f)\chi(v)\ \text{ where } \hat{G}=\mathrm{Hom}(G,\mathbb{C}^*). \tag{2.27}$$

Let us consider the function

$$d:G\to\mathbb{C},\ d(v)=\mathbf{b}'(v)-\mathbf{b}(v).$$

Suppose that (a1) holds. We need to check that (a2) holds, i.e.,

$$\sum_{h\in G}d(h)=0,\quad d(v)=d(-v)\ \forall v\in G.$$

This means that

$$c_{\chi_0}(d)=0$$

and for all *odd characters* χ (i.e., characters χ of g with

$$\chi(-1 \bmod p)=-1)$$

the corresponding *Fourier coefficient*

$$c_\chi(d)=0.$$

It follows from (2.11) that $d*\mathbf{j}(-v)=0$ for all $v\in G$, i.e.,

$$d*\mathbf{j}(v)=0\ \forall v\in G.$$

This implies that

$$0=c_\chi(d*\mathbf{j})=c_\chi(d)\cdot c_\chi(\mathbf{j})\quad \forall\chi\in\hat{G}.$$

However, we know that $c_{\chi_0}(\mathbf{j})\neq 0$. On the other hand, $c_\chi(\mathbf{j})\neq 0$ for all *odd* χ: it follows from [8, Chap. 16, Theorem 2] combined with [11, Ch. 9, p. 288, Thm. 9.9]. This implies that $c_{\chi_0}(d)=0$ and $c_\chi(d)=0$ for all *odd* χ. This proves that (a1) implies (a2). Assume now that (a2) holds. This means that $d(v)$ is an *even* function, i.e.,

$$d(-v)=d(v)\quad \forall v\in G,$$

and

$$\sum_{v\in G} d(v)=0.$$

We need to prove that (a1) holds. Let us prove first that

$$\mathbf{a}(v)=\frac{(p-1)}{p}\cdot \mathbf{b}'*\mathbf{j}_0(-v)+\frac{g}{p-1}\ \forall v\in G. \tag{2.28}$$

In light of (2.22), in order to prove (2.28), it suffices to check that

$$d*\mathbf{j}_0(-v)=0 \quad \forall v\in G,$$

i.e.,

$$D_v:=\sum_{h\in G} d(h)\cdot \mathbf{j}_0(h^{-1}v)=0 \quad \forall v\in G. \tag{2.29}$$

In order to prove (2.29), recall that $\mathbf{j}_0$ is *odd* and d is *even*. This implies that

$$\begin{aligned} D_v &= \sum_{h\in G} d(h)\cdot \mathbf{j}_0(h^{-1}v)=\sum_{h\in G} d(-h)\cdot \mathbf{j}_0((-h)^{-1}v)\\ &= \sum_{h\in G} d(h)\cdot \mathbf{j}_0(-h^{-1}v)=\sum_{h\in G} d(h)\cdot\left(-\mathbf{j}_0(h^{-1}v)\right)=-\sum_{h\in G} d(h)\cdot \mathbf{j}_0(h^{-1}v)=-D_v.\end{aligned}$$

It follows that

$$\sum_{h\in G} d(h)\cdot \mathbf{j}_0(h^{-1}v)=D_v=0,$$

which proves (2.28). Now taking into account that $\mathbf{j}_0=\mathbf{j}-p/2$, we get from (2.28) that

$$\begin{aligned}\mathbf{a}(v) &= \frac{1}{p}\sum_{h\in G}\mathbf{b}'(h)\cdot\left(\mathbf{j}(h^{-1}(-v))-p/2\right)\\ &= \left(\frac{1}{p}\sum_{h\in G}\mathbf{b}'(h)\cdot\mathbf{j}(h^{-1}(-v))\right)-\frac{1}{2}\left(\sum_{h\in G}\mathbf{b}'(h)\right)+\frac{g}{p-1}\\ &= \frac{(p-1)}{p}\cdot\mathbf{b}'*\mathbf{j}(-v)-\frac{1}{2}\left(\frac{2g}{p-1}+2\right)+\frac{g}{p-1}=\mathbf{b}'*\mathbf{j}(-v)-1.\end{aligned}$$

So, $\mathbf{a}(v)=\mathbf{b}'*\mathbf{j}(-v)-1$, i.e., (a1) holds. This ends the proof of (a). Now let $p=3$. Then $2+2g/(p-1)=g+2$ and $G=\{\bar{1}=1 \bmod 3,-\bar{1}\}$. We already know that $\mathbf{b}'(\bar{1})-\mathbf{b}'(-\bar{1})=\mathbf{b}(\bar{1})-\mathbf{b}(-\bar{1})$,

$$\mathbf{b}'(\bar{1})+\mathbf{b}'(-\bar{1})=g+2=\mathbf{b}(\bar{1})+\mathbf{b}(-\bar{1}).$$

This implies that $\mathbf{b}'(\bar{1})=\mathbf{b}(\bar{1}),\quad \mathbf{b}'(-\bar{1})=\mathbf{b}(-\bar{1})$, which proves (b). □

Remark 3. *If $v\in G$ then the positive integer $k_v:=\mathbf{j}(h)$ does* not *divide p and $\mathbf{j}(vh)-k_v\mathbf{j}(h)$ is* divisible *by p for all $h\in G$. Indeed, by definition of $\mathbf{j}$,*

$$v=k_v \bmod p,\quad h=\mathbf{j}(h) \bmod p\in(\mathbb{Z}/p\mathbb{Z})^*=G.$$

This implies that in $(\mathbb{Z}/p\mathbb{Z})^*$ we have

$$\left(k_v\mathbf{j}(h)\right) \bmod p=\left(k_v \bmod p\right)\left(\mathbf{j}(h) \bmod p\right)=vh=\mathbf{j}(vh) \bmod p.$$

Corollary 4. *Let $c:G\to\mathbb{Z}$ be an integer-valued function. Then the following conditions are equivalent.*

(i) $(p-1)\cdot c*\mathbf{j}(1 \bmod p)=\sum_{h\in G}c(h)\mathbf{j}(h^{-1})\in p\mathbb{Z}$.
(ii) $(p-1)\cdot c*\mathbf{j}(v)=\sum_{h\in G}c(h)\mathbf{j}(h^{-1}v)\in p\mathbb{Z}\ \forall v\in G$.

Proof. Clearly, (ii) implies (i). Suppose that (i) holds, i.e.,

$$\sum_{h\in G} c(h)\mathbf{j}(h^{-1}) \in p\mathbb{Z}.$$

In order to prove that (ii) holds, we need to check that

$$\sum_{h\in G} c(h)\mathbf{j}(h^{-1}v) \in p\mathbb{Z}\ \forall v \in G.$$

Notice that in light of Remark 3 (applied to h^{-1}), if $v \in G$ then there exists $k_v \in \mathbb{Z}$ such that $\mathbf{j}(vh^{-1}) - k_v\mathbf{j}(h^{-1})$ is *divisible* by p for all $h \in G$. In other words, $\mathbf{j}(vh^{-1}) \equiv k_v\mathbf{j}(h) \bmod p$. This implies that $\forall v \in G$

$$\sum_{h\in G} c(h)\mathbf{j}(h^{-1}v) = \sum_{h\in G} c(h)\mathbf{j}(vh^{-1}) \equiv k_v \sum_{h\in G} c(h)\mathbf{j}(h^{-1}) \bmod p \equiv 0 \bmod p. \qquad \square$$

The next assertion shows that not every well rounded function is strongly admissible.

Theorem 2.3. *Suppose that* (X,λ) *is the jacobian of a smooth projective irreducible genus* g *curve* $\mathcal{C}$ *with canonical principal polarization, and* δ *is a periodic automorphism of* (X,λ) *that satisfies the* p*th cyclotomic equation. Let*

$$\mathbf{a} = \mathbf{a}_{X,\delta} : G = (\mathbb{Z}/p\mathbb{Z})^* \to \mathbb{Z}_+$$

be the corresponding multiplicity function. Then

$$\frac{1}{p}\cdot\frac{2g}{(p-1)} - \frac{p-2}{p} \le \mathbf{a}(v) \le \frac{2g}{(p-1)} - \left(\frac{1}{p}\cdot\frac{2g}{(p-1)} - \frac{p-2}{p}\right) \quad \forall v \in G. \tag{2.30}$$

In particular, if $(p-2) < 2g/(p-1)$ *then*

$$1 \le \mathbf{a}(v) \le \frac{2g}{p-1} - 1 \quad \forall v \in G.$$

Proof. By Theorem 2.1, there exists a *nonnegative* integer-valued function $\mathbf{b} : G \to \mathbb{Z}_+$ such that

$$\mathbf{a}(h) = \frac{\sum_{u\in G}\mathbf{b}(u)\mathbf{j}(-u^{-1}h)}{p} - 1\ \forall h \in G.$$

Recall that

$$\mathbf{b}(u) \ge 0,\ \sum_{u\in G}\mathbf{b}(u) = \frac{2g}{p-1} + 2,\ \ 1 \le \mathbf{j}(v) \le p-1.$$

This implies that

$$\frac{\sum_{u\in G}\mathbf{b}(u)}{p} - 1 \le \mathbf{a}(h) \le (p-1)\cdot\frac{\sum_{u\in G}\mathbf{b}(u)}{p} - 1.$$

This means that

$$\frac{\frac{2g}{p-1}+2}{p} - 1 \le \mathbf{a}(h) \le (p-1)\cdot\frac{\frac{2g}{p-1}+2}{p} - 1.$$

Hence,

$$\frac{1}{p}\cdot\frac{2g}{(p-1)} - \frac{p-2}{p} \le \mathbf{a}(h) \le \frac{2g}{(p-1)} - \left(\frac{1}{p}\cdot\frac{2g}{(p-1)} - \frac{p-2}{p}\right) \quad \forall v \in G. \qquad \square$$

3. A construction of jacobians

The following theorem may be viewed as an inverse of Theorem 2.1.

Theorem 3.1. *Let g be a positive integer, p an odd prime, $\zeta_p \in \mathbb{C}$ a primitive pth root of unity, and $G = (\mathbb{Z}/p\mathbb{Z})^*$. Suppose that $(p-1)$ divides $2g$. Let $\mathbf{b}: G \to \mathbb{Z}_+$ be a nonnegative integer-valued function such that*

$$\sum_{h\in G} \mathbf{b}(h) = \frac{2g}{p-1} + 2, \tag{3.1}$$

$$(p-1)\cdot \mathbf{b} * \mathbf{j}(1 \bmod p) = \sum_{h\in G} \mathbf{b}(h)\mathbf{j}(h^{-1}) \in p\mathbb{Z}. \tag{3.2}$$

Let $\{f_h(x) \mid h \in G\}$ be a $(p-1)$-element set of mutually prime nonzero polynomials $f_h(x) \in \mathbb{C}[x]$ that enjoy the following properties.

1. $\deg(f_h) = \mathbf{b}(h)$ *for all $h \in G$. In particular, $f_h(x)$ is a (nonzero) constant polynomial if and only if $\mathbf{b}(h) = 0$.*
2. *Each $f_h(x)$ has no repeated roots.*

Let us consider the polynomial

$$f(x) = f_{\mathbf{b}}(x) = \prod_{h\in G} f_h(x)^{\mathbf{j}(h^{-1})} \in \mathbb{C}[x]$$

of degree $\sum_{h\in G} \mathbf{b}(h)\mathbf{j}(h^{-1})$. Let $\mathscr{C}$ be the smooth projective model of the irreducible plane affine curve

$$y^p = f_{\mathbf{b}}(x) \tag{3.3}$$

endowed with an automorphism $\delta_{\mathscr{C}}: \mathscr{C} \to \mathscr{C}$ induced by

$$(x, y) \mapsto (x, \zeta_p y).$$

Let $(\mathscr{J}, \lambda)$ be the canonically principally polarized jacobian of $\mathscr{C}$ endowed by the automorphism δ induced by $\delta_{\mathscr{C}}$. Then $\mathscr{J}$ and δ enjoy the following properties.

(a) $\dim(\mathscr{J}) = g$ *and* $\sum_{j=0}^{p-1} \delta^j = 0$ *in* $\mathrm{End}(\mathscr{J})$.

(b) *Let $\mathbf{a} = \mathbf{a}_{\mathscr{J},\delta}: G \to \mathbb{Z}_+$ be the corresponding multiplicity function defined in* (2.5). *Then for all $v \in G$*

$$\begin{aligned} \mathbf{a}_{\mathscr{J},\delta}(v) &= \frac{(p-1)}{p}\cdot \mathbf{b} * \mathbf{j}(-v) - 1 = \frac{(p-1)}{p}\cdot \mathbf{b} * \mathbf{j}_0(-v) + \frac{g}{p-1} \\ &= \frac{2g}{p-1} - \frac{(p-1)}{p}\cdot \mathbf{b} * \mathbf{j}(v) + 1. \end{aligned} \tag{3.4}$$

Proof of Theorem 3.1. If α is a root of $f(x)$ then there is exactly one $h \in G$ such that α is a root of $f_h(x)$; in addition, the multiplicity of α (viewed as a root of $f(x)$) is $\mathbf{j}(h^{-1})$, which is *not* divisible by p. This implies that $f(x)$ is *not* a pth power in the polynomial ring $\mathbb{C}[x]$ and even in the field of rational functions $\mathbb{C}(x)$. It follows from theorem 9.1 of [9, Ch. VI, Sec. 9] that the polynomial

$$y^p - f(x) \in \mathbb{C}(x)[y]$$

is irreducible over $\mathbb{C}(x)$. This implies that the polynomial in two variables

$$y^p - f(x) \in \mathbb{C}[x, y]$$

is irreducible, because every divisor of it that is a polynomial in x is a constant, i.e., the affine plane curve (3.3) is *irreducible* and its field of rational functions K is the field of fractions of the domain

$$A = \mathbb{C}[x, y]/(y^p - f(x))\mathbb{C}[x, y].$$

Let $\mathscr{C}$ be the smooth projective model of the curve (3.3). Then K is the field $\mathbb{C}(\mathscr{C})$ of rational functions on $\mathscr{C}$; in particular, $\mathbb{C}(\mathscr{C})$ is generated over $\mathbb{C}$ by rational functions x, y. Let $\pi : \mathscr{C} \to \mathbb{P}^1$ be the regular map defined by rational function x. Clearly, it has degree p. Since

$$\deg(\pi) = \deg(f) = \sum_{h\in G} \mathbf{b}(h)\mathbf{j}(h^{-1})$$

is divisible by p, the map π is unramified at ∞ (see [14, Sec. 4]) and therefore the set of branch points of π coincides with the set of roots of $f(x)$, which, in turn, is the disjoint union of the sets R_h of roots of $f_h(x)$. In particular, the number of branch points of π is

$$\sum_{h\in G} \deg(f_h) = \sum_{h\in G} \mathbf{b}(h) = \frac{2g}{p-1} + 2.$$

Clearly, π is a Galois cover of degree p, i.e., the field extension

$$\mathbb{C}(\mathscr{C})/\mathbb{C}(\mathbb{P}^1) = \mathbb{C}(\mathscr{C})/\mathbb{C}(x)$$

is a cyclic field extension of degree p. In addition, the cyclic Galois group

$$\mathrm{Gal}(\mathbb{C}(\mathscr{C})/\mathbb{C}(\mathbb{P}^1))$$

is generated by the automorphism $\delta_{\mathscr{C}} : \mathscr{C} \to \mathscr{C}$ defined by

$$\delta_{\mathscr{C}} : \mathscr{C} \to \mathscr{C},\ (x, y) \mapsto (x, \zeta_p y).$$

It follows from the Riemann-Hurwitz formula (see [14, Sec. 4]) that the genus of $\mathscr{C}$ is

$$\frac{\left(\left(\frac{2g}{p-1} + 2\right) - 2\right)(p-1)}{2} = g.$$

In addition, the automorphism δ of the canonically polarized jacobian $(\mathscr{J}, \lambda)$ induced by $\delta_{\mathscr{C}}$ satisfies the pth cyclotomic equation

$$\sum_{j=0}^{p-1} \delta^j = 0 \in \mathrm{End}(\mathscr{J})$$

(see [14, p. 149]). Let $B \subset \mathscr{C}(\mathbb{C})$ be the set of ramification points of π. Clearly, B coincides with the set of fixed points of $\delta_{\mathscr{C}}$. The map $x : \mathscr{C}(\mathbb{C}) \to \mathbb{P}^1(\mathbb{C})$ establishes a bijection between B and the disjoint union of all R_h's. Let us put

$$B_h = \{P \in B \mid x(P) \in R_h\}.$$

Then B partitions onto a disjoint union of all B_h's and

$$\#(B_h) = \deg(f_h) = \mathbf{b}(h)\ \forall h \in G.$$

Let $P \in B$. The action of δ on the tangent space to $\mathscr{C}$ at P is multiplication by a certain pth root of unity ϵ_P.

Lemma 5. *$\epsilon_P = \zeta_p^{\mathbf{j}(h)}$ if and only if $P \in B_h$.*

Proof of Lemma 5. Clearly, if h_1 and h_2 are *distinct* elements of $G = (\mathbb{Z}/p\mathbb{Z})^*$ then

$$1 \le \mathbf{j}(h_1),\ \mathbf{j}(h_2) \le p-1; \quad \mathbf{j}(h_1) \ne \mathbf{j}(h_2).$$

Therefore $\zeta_p^{\mathbf{j}(h_1)} \ne \zeta_p^{\mathbf{j}(h_2)}$. Hence, in order to prove our lemma, it suffices to check that

$$\epsilon_P = \zeta_p^{\mathbf{j}(h)} \text{ if } P \in B_h. \tag{3.5}$$

So, let $P \in B_h$. Then we have

$$x(P) = \alpha \in R_h,\ y(P) = 0.$$

Let

$$\mathrm{ord}_P : \mathbb{C}(\mathscr{C}) \twoheadrightarrow \mathbb{Z}$$

be the discrete valuation map attached to P. Then one may easily check that

$$\mathrm{ord}_P(x-\alpha)=p,\ \mathrm{ord}_P(x-\beta)=0\ \forall\beta\in\mathbb{C}\setminus\{\alpha\}.$$

This implies that

$$\mathbf{j}(h^{-1})\cdot\mathrm{ord}_P(x-\alpha)=\mathrm{ord}_P(y^p)=p\cdot\mathrm{ord}_P(y)$$

and therefore

$$\mathrm{ord}_P(y)=\mathbf{j}(h^{-1}). \tag{3.6}$$

In light of (2.8), there is an integer m such that

$$\mathbf{j}(h^{-1})\cdot\mathbf{j}(h)=1+pm.$$

Combining this with (3.6), we obtain that

$$\mathrm{ord}_P\left(\frac{y^{\mathbf{j}(h)}}{(x-\alpha)^m}\right)=\mathbf{j}(h^{-1})\cdot\mathbf{j}(h)-pm=1$$

and therefore $t:=y^{\mathbf{j}(h)}/(x-\alpha)^m$ is a *local parameter* of $\mathscr{C}$ at P. Clearly, the action of δ multiplies t by $\zeta_p^{\mathbf{j}(h)}$ and therefore $\epsilon_P=\zeta_p^{\mathbf{j}(h)}$, which proves the lemma. □

End of Proof of Theorem 3.1. Now the desired result follows from Proposition 2.2 applied to $X=\mathscr{J},\phi=\delta$ combined with (2.28) and (2.24). □

4. The $p=3$ case

Throughout this this section we assume that $p=3$ (see also [21]). We have seen (Example 1) that every well rounded function of degree g is admissible and the number of such functions is $(g+1)$. We have

$$G=(\mathbb{Z}/3\mathbb{Z})^*=\{\bar{1}=1\bmod 3,\ \bar{2}=2\bmod 3=-\bar{1}\}.$$

Remark 4. *Let* $\mathbf{b}:G\to\mathbb{Z}_+$ *be a nonnegative integer valued function such that*

$$\mathbf{b}(\bar{1})+\mathbf{b}(\bar{2})=g+2,\quad \mathbf{b}(\bar{1})+2\mathbf{b}(\bar{2})\in 3\mathbb{Z}.$$

It follows from Theorem 2.1 and (3.4) *that both*

$$a_1=(g+1)-\frac{\mathbf{b}(\bar{1})+2\mathbf{b}(\bar{2})}{3}\quad\textit{and}\quad a_2=(g+1)-\frac{2\mathbf{b}(\bar{1})+\mathbf{b}(\bar{2})}{3}$$

are nonnegative integers, and the function

$$\mathscr{F}_{\mathbf{b}}:G\to\mathbb{Z}_+,\ \ \bar{1}\mapsto a_1,\ \ \bar{2}=-\bar{1}\mapsto a_2$$

is strongly admissible.

Now let us list explicitly all strongly admissible functions. (Essentially, such a list has appeared in [1, Lemma 2.9].)

Theorem 4.1. *Let* $\mathbf{a}:G\to\mathbb{Z}_+$ *be a nonnegative integer valued function such that*

$$\mathbf{a}(\bar{1})+\mathbf{a}(\bar{2})=g, \tag{4.1}$$

i.e., $\mathbf{a}$ *is well rounded.*

Then $\mathbf{a}$ *is strongly admissible if and only if*

$$\frac{g-1}{3}\le\mathbf{a}(\bar{1}),\ \mathbf{a}(\bar{2})\le\frac{2g+1}{3}. \tag{4.2}$$

Remark 5. *Clearly, if* $\mathbf{a}$ *is well rounded then* $\mathbf{a}(\bar{1})$ *satisfies the inequalities* (4.2) *if and only if* $\mathbf{a}(\bar{2})$ *satisfies them. This implies that the number of strongly admissible functions of degree* g *equals the number of integers* a *such that*

$$\frac{g-1}{3} \le a \le \frac{2g+1}{3}. \tag{4.3}$$

Indeed, let us attach to such a *the well rounded function* $\mathbf{a}: G \to \mathbb{Z}_+$ *defined by*

$$\mathbf{a}(\bar{1}) := a \ge \frac{g-1}{3}, \quad \mathbf{a}(\bar{2}) := g - \mathbf{a}(1) = g - a \le g - \frac{g-1}{3} = \frac{2g+1}{3}; \tag{4.4}$$

in addition,

$$\mathbf{a}(\bar{2}) = g - a \ge g - \frac{2g+1}{3} = \frac{g-1}{3}.$$

By Theorem 4.1, $\mathbf{a}$ *is strongly admissible. Conversely, every strongly admissible function* $\mathbf{a}$ *is uniquely determined (as in* (4.4)*) by an integer* $a := \mathbf{a}(\bar{1})$ *that satisfies the inequalities* (4.3).

Proof of Theorem 4.1. It follows from Theorem 2.3 applied to $p = 3$ that every strongly admissible function $\mathbf{a}$ of degree g enjoys properties (4.2).

Conversely, suppose that $\mathbf{a}$ is well rounded function of degree g that enjoy properties (4.2). Let us consider the integers

$$b_1 := (2g+1) - 3\mathbf{a}(\bar{1}), \quad b_2 := 3\mathbf{a}(\bar{1}) - (g-1).$$

It follows from (4.2) that both b_1 and b_2 are *nonnegative* integers. In addition,

$$b_1 + b_2 = \big((2g+1) - 3\mathbf{a}(\bar{1})\big) + \big(3\mathbf{a}(\bar{1}) - (g-1)\big) = (2g+1) - (g-1) = g+2;$$
$$b_1 + 2b_2 = 2\big((2g+1) - 3\mathbf{a}(\bar{1})\big) + \big(3\mathbf{a}(\bar{1}) - (g-1)\big) = (3g+3) - 3\mathbf{a}(\bar{1}).$$

Hence, b_1 and b_2 are nonnegative integers such that

$$b_1 + b_2 = g+2, \quad b_1 + 2b_2 = (3g+3) - 3\mathbf{a}(\bar{1}) = 3\big(g+1-\mathbf{a}(\bar{1})\big) \in 3\mathbb{Z}.$$

It follows from Remark 4 that if we consider the function

$$\mathbf{b}: G \to \mathbb{Z}_+, \quad \bar{1} \mapsto b_1,\ \bar{2} \mapsto b_2,$$

then the function

$$\mathscr{F}_{\mathbf{b}}: G \to \mathbb{Z}_+, \quad \bar{1} \mapsto (g+1) - \frac{\mathbf{b}(\bar{1}) + 2\mathbf{b}(\bar{2})}{3},\ \bar{2} \mapsto (g+1) - \frac{2\mathbf{b}(\bar{1}) + \mathbf{b}(\bar{2})}{3}$$

is strongly admissible; in particular, it is well rounded. We have

$$\mathscr{F}_{\mathbf{b}}(\bar{1}) = (g+1) - \frac{\mathbf{b}(\bar{1}) + 2\mathbf{b}(\bar{2})}{3} = (g+1) - \frac{3\big(g+1-\mathbf{a}(\bar{1})\big)}{3} = (g+1) - (g+1-\mathbf{a}(\bar{1})) = \mathbf{a}(\bar{1}).$$

Since $\mathscr{F}_{\mathbf{b}}$ is well rounded,

$$\mathscr{F}_{\mathbf{b}}(\bar{2}) = \mathscr{F}_{\mathbf{b}}(-\bar{1}) = g - \mathscr{F}_{\mathbf{b}}(\bar{1}) = g - \mathbf{a}(\bar{1}) = \mathbf{a}(-\bar{1}) = \mathbf{a}(\bar{2}).$$

This implies that the function $\mathbf{a}$ coincides with the strongly admissible function $\mathscr{F}_{\mathbf{b}}$ and therefore is strongly admissible itself. This ends the proof. □

We finish this section by counting the number $A_3(g)$ of strongly admissible functions of degree g, using Remark 5.

(1) If $g = 3k+1$ where k is a nonnegative integer. then $A_3(3k+1)$ is the number of integers a with

$$k = \frac{g-1}{3} \le a \le \frac{2g+1}{3} = \frac{6k+3}{3} = 2k+1.$$

Hence, $A_3(3k+1) = k+2$.

(2) If $g = 3k+2$ where k is a nonnegative integer. then $A_3(3k+2)$ is the number of integers a with

$$k+1/3 = \frac{g-1}{3} \le a \le \frac{2g+1}{3} = \frac{6k+4}{3} = 2k+1+1/3.$$

Hence, $A_3(3k+2) = k+1$.

(3) If $g = 3k$ where k is a positive integer then $A_3(3k)$ is the number of integers a with

$$k-1/3 = \frac{g-1}{3} \le a \le \frac{2g+1}{3} = \frac{6k+1}{3} = 2k+1/3.$$

Hence, $A_3(3k) = k+1$.

5. The CM case

We use the notation and assumptions of Section 2. Suppose that $\dim(X) = g = (p-1)/2$, i.e. $2g = (p-1)$. Then X becomes an abelian variety of CM type with multiplication by the CM field $\mathbb{Q}(\zeta_p)$ of degree $(p-1)$. The corresponding nonnegative multiplicity function $\mathbf{a}_{X,\delta}$ enjoys the property

$$\mathbf{a}_{X,\delta}(h) + \mathbf{a}_{X,\delta}(-h) = \frac{2g}{p-1} = 1,$$

which means that for each $h \in G$ either

$$\mathbf{a}_{X,\delta}(h) = 1, \quad \mathbf{a}_{X,\delta}(-h) = 0$$

or

$$\mathbf{a}_{X,\delta}(h) = 0, \quad \mathbf{a}_{X,\delta}(-h) = 1.$$

To each $h \in G = (\mathbb{Z}/p\mathbb{Z})^*$ corresponds the field embedding

$$\psi_h : \mathbb{Q}(\zeta_p) \to \mathbb{C},\ \zeta_p \mapsto \zeta_p^h.$$

Clearly, the CM type of X is the $(p-1)/2$-element set

$$\Psi = \Psi_{X,\delta} = \{\psi_h \mid \mathbf{a}_{X,\delta}(h) = 1\}.$$

Example 3. *Let $\mathscr{C}$ be the smooth projective model of the plane affine curve $y^2 = 1 - x^p$. Then $\mathscr{C}$ has genus $g = (p-1)/2$ and admits an automorphism $\delta_{\mathscr{C}} : \mathscr{C} \to \mathscr{C}$ induced by*

$$(x, y) \mapsto (\zeta_p x, y).$$

Let $(\mathscr{J}, \lambda)$ be the canonically principally polarized jacobian of $\mathscr{C}$ endowed by the automorphism $\delta \in \mathrm{Aut}(\mathscr{J}, \lambda)$ induced by $\delta_{\mathscr{C}}$. It is known [17, Example 15.4(2)] *that $\zeta_p \to \delta$ can be extended to the ring homomorphism $\mathbb{Z}[\zeta_p] \to \mathrm{End}(\mathscr{J})$ (i.e., $\sum_{i=0}^{p-1} \delta^i = 0$), which makes $\mathscr{J}$ an abelian variety of CM type with multiplication by $\mathbb{Q}(\zeta_p)$ and its CM type Ψ is $\{\psi_i \mid 1 \le i \le g = (p-1)/2\}$. This means that the corresponding multiplicity function $\mathbf{a}_{\mathscr{J},\delta}(h)$ is as follows:*

$$\mathbf{a}_{\mathscr{J},\delta}(i \bmod p) = 1 \ \text{ if } 1 \le i \le (p-1)/2;$$
$$\mathbf{a}_{\mathscr{J},\delta}(i \bmod p) = 0 \ \text{ if } i > (p-1)/2.$$

Recall that p is an odd prime. The case $p = 3$ (with arbitrary g) was discussed in detail in Section 4. The following assertion deals with $p > 3$ when $g = (p-1)/2$.

Theorem 5.1. *Let $p > 3$ and $g = (p-1)/2$. Then the number of strongly admissible functions of degree g is $(p^2-1)/6$. In particular, every well rounded function of degree g is strongly admissible if and only if $p \in \{5, 7\}$.*

Proof. So, we need to compute the number of strongly admissible functions when $2g = p-1$. By Theorem 2.1, each strongly admissible function is of the form $\frac{(p-1)}{p}\cdot \mathbf{b}*\mathbf{j}(-v)-1$ where the nonnegative integer-valued function $\mathbf{b}: G\to\mathbb{Z}_+$ enjoys the properties

$$\sum_{h\in G}\mathbf{b}(h)=\frac{2g}{p-1}+2=1+2=3; \tag{5.1}$$

$$\sum_{h\in G}\mathbf{b}(h)\mathbf{j}(h^{-1})\in p\mathbb{Z}. \tag{5.2}$$

Taking into account that

$$1\le \mathbf{j}(h^{-1})<p \quad \forall h\in G,$$

we conclude that

$$\sum_{h\in G}\mathbf{b}(h)\mathbf{j}(h^{-1})<\left(\sum_{h\in G}\mathbf{b}(h)\right)p=3p.$$

Hence, (5.2) means that either

$$\sum_{h\in G}\mathbf{b}(h)\mathbf{j}(h^{-1})=p \tag{5.3}$$

or

$$\sum_{h\in G}\mathbf{b}(h)\mathbf{j}(h^{-1})=2p. \tag{5.4}$$

Let us compute the number of functions $\mathbf{b}$ that enjoy either properties (5.1) and (5.3) or properties (5.1) and (5.4). First, let us prove that

$$\mathbf{b}(h)\in\{0,1,2\}\ \forall h\in G. \tag{5.5}$$

Indeed, it follows readily from (5.1) that

$$\mathbf{b}(h)\in\{0,1,2,3\}\ \forall h\in G.$$

Suppose that $\mathbf{b}(v)=3$ for some $v\in G$. Then it follows from (5.1) that all other values of $\mathbf{b}$ are zeros. Now (5.2) implies that

$$3\cdot\mathbf{j}(v^{-1})=\mathbf{b}(v)\mathbf{j}(v^{-1})=\sum_{h\in G}\mathbf{b}(h)\mathbf{j}(h^{-1})\in p\mathbb{Z}.$$

Since a positive integer $\mathbf{j}(v^{-1})$ is strictly less than p, the prime p must divide 3, which is not true, because $p>3$. The obtained contradiction proves (5.5).

Now notice that

$$\mathbf{j}(v)+\mathbf{j}(-v)=p\ \forall v\in G \tag{5.6}$$

(it follows readily from the very definition of $\mathbf{j}$). Let us consider the function

$$\bar{\mathbf{b}}: G\to\mathbb{Z}_+,\ h\mapsto\mathbf{b}(-h). \tag{5.7}$$

Clearly,

$$\sum_{h\in G}\bar{\mathbf{b}}(h)=\sum_{h\in G}\mathbf{b}(h)=3;\quad \bar{\mathbf{b}}(G)=\mathbf{b}(G)\subset\{0,1,2\}.$$

On the other hand,

$$\sum_{h\in G}\bar{\mathbf{b}}(h)\mathbf{j}(h^{-1})=\sum_{h\in G}\mathbf{b}(-h)\mathbf{j}(h^{-1})=\sum_{h\in G}\mathbf{b}(h)\mathbf{j}(-h^{-1})=\sum_{h\in G}\mathbf{b}(h)\left(p-\mathbf{j}(h^{-1})\right)$$
$$=p\left(\sum_{h\in G}\mathbf{b}(h)\right)-\left(\sum_{h\in G}\mathbf{b}(h)\mathbf{j}(h^{-1})\right)=3p-\left(\sum_{h\in G}\mathbf{b}(h)\mathbf{j}(h^{-1})\right).$$

It follows that

$$\sum_{h\in G}\bar{\mathbf{b}}(h)\mathbf{j}(h^{-1})=3p-p=2p$$

if **b** satisfies (5.3). On the other hand, if **b** satisfies (5.4) then

$$\sum_{h\in G} \bar{\mathbf{b}}(h)\mathbf{j}(h^{-1}) = 3p-2p = p.$$

It follows from Theorem 3.1 combined with Remark 1(iii) that

$$h \mapsto \bar{\mathbf{a}}(h) = \mathbf{a}(-h) = \frac{2g}{p-1} - \mathbf{a}(h) = 1-\mathbf{a}(h)$$

is a strongly admissible function of degree $g=(p-1)/2$. This implies that $\mathbf{a}(1 \bmod p)=1$ (resp. 0) if and only if $\bar{\mathbf{a}}(1 \bmod p)=0$ (resp. 1).

Notice that

$$\mathbf{a}(-1 \bmod p) = \frac{\sum_{h\in G}\mathbf{b}(h)\mathbf{j}(h^{-1})}{p} - 1.$$

This implies that $\mathbf{a}(1 \bmod p)=1$ (resp. 0) if and only if $\sum_{h\in G}\mathbf{b}(h)\mathbf{j}(h^{-1})=p$ (resp. $2p$).

We will need the following two auxiliary assertions.

Lemma 6. *Let $Q_3(p)$ be the set of partitions in 3 parts of p.*

There is a natural bijection between $Q_3(p)$ and the set of strongly admissible functions $\mathbf{a}: G \to \mathbb{Z}_+$ of degree $g=(p-1)/2$ such that

$$\mathbf{a}(1 \bmod p) = 1.$$

Lemma 7. *The cardinality of $Q_3(p)$ is $(p^2-1)/12$.*

End of proof of Theorem 5.1 (*modulo Lemmas 6 and 7*). The map $\mathbf{a} \mapsto \bar{\mathbf{a}}$ is a bijection between the sets of strongly admissible functions that take on at 1 mod p the values 0 and 1 respectively. Applying both lemmas, we conclude that the number of all strongly admissible functions functions of degree $(p-1)/2$ is twice the cardinality of $Q_3(p)$, i.e., this number is

$$2\cdot\frac{p^2-1}{12} = \frac{p^2-1}{6},$$

which proves first assertion of Theorem 5.1. As for the second one, recall that the number of well rounded functions of degree $(p-1)/2$ is $2^{(p-1)/2}$. It remains to notice that $2^{(p-1)/2} > (p^2-1)/6$ if $p \ge 11$ while $2^{(p-1)/2} = (p^2-1)/6$ if $p \in \{5,7\}$. □

Proof of Lemma 6. If $v \in G$ then we write $\delta_v : G \to \mathbb{Z}_+$ for the corresponding *delta function* that takes on value 1 at v and vanishes elsewhere.

Each element M of $Q_3(p)$ may be viewed as an unordered triple $\{m_1, m_2, m_3\}$ of positive integers whose sum $\sum_{i=1}^3 m_i = p$. Clearly,

$$p > m_i \ne p - m_j \quad \forall i,j \in \{1,2,3\}.$$

Let us define

$$h_i := (m_i \bmod p)^{-1} \in (\mathbb{Z}/p\mathbb{Z})^* = G.$$

Clearly,

$$h_i^{-1} = m_i \bmod p,\ \ \mathbf{j}(h_i^{-1}) = m_i,\ \ h_i^{-1} \ne -h_j^{-1} \quad \forall i,j = 1,2,3. \tag{5.8}$$

Let us consider the function

$$\mathbf{b}_M = \sum_{i=1}^3 \delta_{h_i} : G \to \mathbb{Z}_+.$$

We have

$$\sum_{h\in G}\mathbf{b}_M(h) = \sum_{i=1}^3\left(\sum_{h\in G}\delta_{h_i}(h)\right) = \sum_{i=1}^3 1 = 3,$$

$$\sum_{h\in G}\mathbf{b}_M(h)\mathbf{j}(h^{-1}) = \sum_{i=1}^3\left(\sum_{h\in G}\delta_{h_i}(h)\mathbf{j}(h^{-1})\right) = \sum_{i=1}^3 \mathbf{j}(h_i^{-1}) = \sum_{i=1}^3 m_i = p.$$

By Theorem 3.1, the function

$$\mathbf{a}_M : G \to \mathbb{Z}_+, \ \ v \mapsto \frac{p-1}{p} b_M * \mathbf{j}(-v) - 1 = \frac{\sum_{h\in G} b_M(h)\mathbf{j}(-h^{-1}v)}{p} - 1$$

is strongly admissible; in addition,

$$\mathbf{a}_M(1 \bmod p) = \frac{2g}{p-1} - \mathbf{a}_M(-1 \bmod p) = 1 - \left(\frac{\sum_{h\in G} b_M(h)\mathbf{j}(h^{-1})}{p} - 1\right) = 1 - \left(\frac{p}{p} - 1\right) = 1.$$

Let us consider the map

$$\mathcal{T} : M \to \mathbf{a}_M$$

from $Q_3(p)$ to the set of strongly admissible functions $G \to \mathbb{Z}_+$ of degree $(p-1)/2$ that take on value 1 at 1 mod p. Let us check that $\mathcal{T}$ is *bijective*. In order to check the injectiveness of $\mathcal{T}$, notice that in light of the last inequality of (5.8)

$$\mathbf{b}_M(h) = \max\{\mathbf{b}_M(h) - \mathbf{b}_M(-h),\ 0\},$$

which means that the function $\mathbf{b}_M(h)$ is uniquely determined by its “odd part”. It follows from Corollary 3 that $\mathcal{T}$ is *injective*. In order to check that $\mathcal{T}$ is *surjective*, let us start with a strongly admissible function $\mathbf{a} : G \to \mathbb{Z}_+$ of degree $(p-1)/2$ with $\mathbf{a}(1 \bmod p) = 1$. We know that there is a function

$$\mathbf{b} : G \to \{0,1,2\} \subset \mathbb{Z}_+$$

such that

$$\sum_{h\in G} \mathbf{b}(h) = 3, \quad \sum_{h\in G} b(h)\mathbf{j}(h^{-1}) = p \tag{5.9}$$

and

$$\mathbf{a}(v) = \frac{p-1}{p}\mathbf{b} * \mathbf{j}(-v) - 1 = \frac{\sum_{h\in G} b(h)\mathbf{j}(-h^{-1}v)}{p} - 1 \ \forall v \in G.$$

We need to find a partition M of p in three parts such that $\mathbf{b} = \mathbf{b}_M$ (which would imply that $\mathbf{a} = \mathbf{a}_M$). Recall that $\mathbf{b}$ is a nonnnegative integer-valued function. In light of of first equality of (5.9), there is a 3-element collection $\{h_1, h_2, h_3\}$ of (not necessarily distinct) elements of G such that

$$\mathbf{b} = \delta_{h_3} + \delta_{h_2} + \delta_{h_1}.$$

Let us define the 3-element collection

$$M := \{m_1 = \mathbf{j}(h_1^{-1}),\ m_2 = \mathbf{j}(h_2^{-1}),\ m_3 = \mathbf{j}(h_3^{-1})\}$$

of (not necessarily distinct) positive integers. In light of second equality of (5.9),

$$p = \sum_{h\in G} b(h)\mathbf{j}(h^{-1}) = \sum_{i=1}^{3} \mathbf{j}(h_i^{-1}) = m_1 + m_2 + m_3,$$

i.e., M is a partition of p in three parts. Clearly, we have $\mathbf{b} = \mathbf{b}_M$ and therefore $\mathbf{a} = \mathbf{a}_M$, which proves the surjectiveness of $\mathcal{T}$. □

Proof of Lemma 7. We know that the prime $p > 3$ is congruent to ± 1 modulo 6. This implies a well known assertion that $p^2 - 1$ is divisible by 12 (and even by 24). This implies that $(p^2-1)/12$ is the *nearest integer* to $p^2/12$.

It is well known [2, Sec. 3.1, p. 16] that the cardinality $\#(Q_3(p))$ of $Q_3(p)$ coincides with the number of partitions of $p-3$ in at most three parts. On the other hand, it is known [2, Sec. 6.2, p. 58] that the latter number is the nearest integer to $\frac{((p-3)+3)^2}{12}$, i.e., is the nearest integer to $p^2/12$, which (as we have already seen) is $(p^2-1)/12$. This ends the proof of Lemma 7. □

6. Self-products of abelian varieties that are not jacobians

Let us start by recalling some generalities about endomorphism algebras of abelian varieties and Rosati (anti-)involutions [13, Sec. 19–21].

Let X be a positive-dimensional abelian variety over an arbitrary algebraically closed field, $\mathrm{End}(X)$ its endomorphism ring and $\mathcal{Z}_X$ the center of of $\mathrm{End}(X)$. Then $\mathcal{Z}_X^0=\mathcal{Z}_X\otimes\mathbb{Q}$ is the center of the endomorphism algebra $\mathrm{End}^0(X):=\mathrm{End}(X)\otimes\mathbb{Q}$; the latter is a finite-dimensional semisimple $\mathbb{Q}$-algebra [13, Sec. 19, Cor. 2]. More precisely, there is an isomorphism of $\mathbb{Q}$-algebras

$$\mathrm{End}^0(X)\cong\oplus_{i=1}^{\ell}\mathcal{H}_i=:\mathcal{H}$$

where ℓ is a certain positive integer and each $\mathcal{H}_i$ is a central simple algebra over a number field K_i of dimension d_i^2, where d_i is a positive integer while K_i is either totally real or a CM field [13, Sec. 21, Application I]. In what follows, we will identify $\mathrm{End}^0(X)$ with $\mathcal{H}$ and will view each direct summand $\mathcal{H}_i$ as the corresponding two-sided ideal of $\mathcal{H}$. Then

$$\mathcal{Z}_X^0=\oplus_{i=1}^{\ell}K_i\subset\oplus_{i=1}^{\ell}\mathcal{H}_i=\mathcal{H}.$$

We write e_i for the identity element of $\mathcal{H}_i$, viewed as the certain idempotent of $\mathrm{End}^0(X)$. Clearly,

$$e_i\in e_i\mathcal{Z}_X^0=K_i\subset\mathcal{H}_i=e_i\mathrm{End}^0(X)=\mathrm{End}^0(X)e_i;$$

$$e_ie_j=0\ \ \forall i\ne j;\quad \sum_{i=1}^{\ell}e_i=1\in\mathcal{H}.$$

In addition, $\{e_1,\dots e_\ell\}$ is the list of all minimal idempotents in $\mathcal{Z}_X^0$.

One may view $\mathrm{End}(X)$ and $\mathcal{Z}_X$ as orders in $\mathrm{End}^0(X)=\mathcal{H}$ and $\mathcal{Z}_X^0$ respectively.

We write $\mathrm{tr}_{\mathcal{H}_i/K_i}:\mathcal{H}_i\to K_i$ for the K_i-linear *reduced trace* map of the central simple K_i-algebra $\mathcal{H}_i$ over K_i [15, Ch. 2, Subsec. 9a]. Recall its definition and basic properties. Let E_i be an overfield of K_i that splits $\mathcal{H}_i$. There exists an isomorphism

$$h_i:\mathcal{H}_i\otimes_{K_i}E_i\cong\mathrm{Mat}_{d_i}(E_i)$$

of central simple E_i-algebras (where $\mathrm{Mat}_{d_i}(E_i)$ is the algebra of square matrices of size d_i with entries in E_i). Then for all $u_i\in\mathcal{H}_i$, one defines $\mathrm{tr}_{\mathcal{H}_i/K_i}(u_i)$ as the trace of the matrix $h_i(u_i\otimes 1)$; this trace lies in K_i and does *not* depend on the choice of E_i and h_i. E.g., if $u_i\in K_i\subset\mathcal{H}_i$ then $h_i(u\otimes 1)$ is the *scalar matrix* $u_i\mathrm{I}_{d_i}$ where I_{d_i} is the identity matrix in $\mathrm{Mat}_{d_i}(E_i)$. The trace of the scalar matrix $u_i\mathrm{I}_{d_i}$ is obviously d_iu_i, which implies that $\mathrm{tr}_{\mathcal{H}_i/K_i}$ coincides with multiplication by d_i on K_i. We also have

$$\mathrm{tr}_{\mathcal{H}_i/K_i}(u_iv_i)=\mathrm{tr}_{\mathcal{H}_i/K_i}(v_iu_i)\quad\forall u_i,v_i\in\mathcal{H}_i.$$

We write

$$\mathrm{tr}_{\mathcal{H}/\mathbb{Q}}:\mathcal{H}=\oplus_{i=1}^{\ell}\mathcal{H}_i\to\mathbb{Q}$$

for the *reduced trace map* on the $\mathbb{Q}$-algebra $\mathcal{H}$, which is defined as

$$(u_1,\dots,u_\ell)\mapsto\sum_{i=1}^{\ell}\mathrm{Tr}_{K_i/\mathbb{Q}}(\mathrm{tr}_{\mathcal{H}_i/K_i}(u_i))\qquad\text{where }\ u_i\in\mathcal{H}_i\ \ \forall i,$$

and $\mathrm{Tr}_{K_i/\mathbb{Q}}:K_i\to\mathbb{Q}$ is the usual trace map attached to the field extension $K_i/\mathbb{Q}$ [15, Ch. 2, Subsec. 9b]. Clearly, $\mathrm{tr}_{\mathcal{H}/\mathbb{Q}}$ coincides with the composition $\mathrm{Tr}_{K_i/\mathbb{Q}}\circ\mathrm{tr}_{\mathcal{H}_i/K_i}$ on $\mathcal{H}_i\subset\mathcal{H}$ and therefore coincides with $d_i\cdot\mathrm{Tr}_{K_i/\mathbb{Q}}$ on K_i. It is also clear that $\mathrm{tr}_{\mathcal{H}/\mathbb{Q}}$ is a $\mathbb{Q}$-linear map such that

$$\mathrm{tr}_{\mathcal{H}/\mathbb{Q}}(uv)=\mathrm{tr}_{\mathcal{H}/\mathbb{Q}}(vu)\quad\forall u,v\in\mathcal{H}.$$

If λ is a polarization on X then it gives rise to the so called *Rosati involution* (actually, anti-involution)

$$\mathrm{End}^0(X) \to \mathrm{End}(X),\ u \mapsto u^*,\ (u^*)^* = u,\ (uv)^* = v^* u^*\ \forall u, v \in \mathrm{End}^0(X) = \mathcal{H},$$

which is a $\mathbb{Q}$-linear map [13, Sec. 20]. The Rosati involution is *positive* [13, Sec. 21], i.e.,

$$\mathrm{tr}_{\mathcal{H}/\mathbb{Q}}(uu^*) = \mathrm{tr}_{\mathcal{H}/\mathbb{Q}}(u^* u) > 0 \quad \forall \text{ nonzero } u \in \mathcal{H}.$$

Clearly, this involution defines an automorphism (an honest involution)

$$\mathcal{Z}_X^0 \to \mathcal{Z}_X^0,\ u \to u^* \tag{6.1}$$

of the commutative semisimple $\mathbb{Q}$-algebra $\mathcal{Z}_X$. It follows that the Rosati involution permutes the set of minimal idempotents $\{e_1, \dots e_\ell\}$. On the other hand, if $e_i^* = e_j$ with $j \ne i$ then $e_i e_j = 0$, hence,

$$\mathrm{tr}_{\mathcal{H}/\mathbb{Q}}(e_i e_i^*) = \mathrm{tr}_{\mathcal{H}/\mathbb{Q}}(e_i e_j) = \mathrm{tr}_{\mathcal{H}/\mathbb{Q}}(0) = 0,$$

which contradicts the positivity of the Rosati involution. Hence, $e_i^* = e_i$ for all i. It follows that the Rosati involution sends $\mathcal{H}_i = e_i\mathcal{H}$ to $\mathcal{H} e_i = \mathcal{H}_i$, i.e., $\mathcal{H}_i$ goes to itself under this involution. This implies that the center K_i of $\mathcal{H}_i$ goes to itself under this involution. The positiveness of the Rosati involution on $\mathcal{H}$ implies that for all *nonzero* $u \in K_i$

$$d_i \cdot \mathrm{Tr}_{K_i/\mathbb{Q}}(uu^*) > 0, \text{ i.e. } \mathrm{Tr}_{K_i/\mathbb{Q}}(uu^*) > 0.$$

It follows that $u \mapsto u^*$ is a positive involution on K_i. By Albert's classification [13, Sec. 21, Application I], this involution acts on K_i as the identity map if K_i is totally real and as the complex conjugation if K_i is a CM field. This implies the $\mathbb{Q}$-algebra automorphism (6.1) of the center does *not* depend on the choice of the polarization λ.

On the other hand, if u is automorphism of X then $u \in \mathrm{Aut}(X, \lambda)$ if and only if $u^* u = 1_X$ [13, Definition in Sec. 8 and Sec. 21, proof of Thm. 5, first paragraph]. (Over $\mathbb{C}$ this well known assertion follows readily from the very definition of Rosati involution [4, Sec. 5.1, p. 114] combined with the commutative diagram in [4, Cor. 2.4.6 on p. 36].) It follows that if $u \in \mathcal{Z}_X$ respects one polarization on X then it respects all of them!

Now let us return to our study of complex abelian varieties with automorphisms that satisfy the pth cyclotomic equation.

Theorem 6.1. *Let p be an odd prime, g a positive integer such that $(p-1)$ divides $2g$, X a complex g-dimensional abelian variety endowed with the ring embeddings*

$$\kappa : \mathbb{Z}[\zeta_p] \hookrightarrow \mathcal{Z}_X \subset \mathrm{End}(X),\ 1 \mapsto 1_X$$

where $\mathcal{Z}_X$ is the center of $\mathrm{End}(X)$. *Let us put*

$$\delta := \kappa(\zeta_p) \in \mathcal{Z}_X \subset \mathrm{End}(X).$$

If X is isomorphic as an algebraic variety to the jacobian of a smooth connected projective curve of genus g then it enjoys one of the following two properties.

(i)
$$\frac{2g}{p-1} \le p-2.$$

(ii) *Every primitive pth root of unity ζ is an eigenvalue of $\delta_\Omega : \Omega^1(X) \to \Omega^1(X)$ and its multiplicity is greater or equal than*

$$\frac{1}{p} \cdot \frac{2g}{p-1} - \frac{p-2}{p}.$$

Proof. Clearly, κ extends by $\mathbb{Q}$-linearity to the embedding of $\mathbb{Q}$-algebras

$$\mathbb{Q}(\zeta_p) \hookrightarrow \mathcal{Z}_X \subset \mathrm{End}^0(X), \quad 1 \mapsto 1_X,\ \zeta_p \mapsto \delta,$$

which we continue to denote by κ. Since $\mathbb{Q}(\zeta_p)$ is a CM field, the center $\mathcal{Z}_X$ is either a CM field or a product of CM fields, and (as we have seen in Section 6) the Rosati involution coincides with the complex conjugation on each factor. It follows that

$$\kappa(\bar{u}) = (\kappa(u))^* \quad \forall u \in \mathbb{Q}(\zeta_p).$$

(Here $\bar{u}$ is the complex-conjugate of u.) Taking into account that $\bar{\zeta_p}\zeta_p = 1$ (where $\bar{\zeta_p}$ is the complex-conjugate of ζ_p), we conclude that

$$\delta^*\delta = \kappa\left(\bar{\zeta_p}\right)\kappa(\zeta_p) = \kappa\left(\bar{\zeta_p}\zeta_p\right) = \kappa(1) = 1_X,$$

i.e., $\delta^*\delta = 1_X$, which means that $\delta \in \mathrm{Aut}(X,\lambda)$ for any polarization λ on X. Now the desired result follows from Theorem 2.3. □

Corollary 5. *Let p be an odd prime, g_0 a positive integer such that $(p-1)$ divides $2g_0$. Let Y be a complex g_0-dimensional abelian variety endowed with the ring embeddings*

$$\kappa : \mathbb{Z}[\zeta_p] \hookrightarrow \mathcal{Z}_Y \subset \mathrm{End}(Y),\ 1 \mapsto 1_Y.$$

Let us put

$$\delta_Y := \kappa(\zeta_p) \in \mathcal{Z}_Y \subset \mathrm{End}(Y).$$

Suppose that there is a primitive pth root of unity ζ that enjoys one of the following two properties.

(i) *ζ is not an eigenvalue of $\delta_{Y,\Omega} : \Omega^1(X) \to \Omega^1(X)$.*

(ii) *ζ is an eigenvalue of $\delta_{Y,\Omega}$ but its multiplicity a is strictly less than*

$$\frac{1}{p}\cdot\frac{2g_0}{p-1}.$$

Then the self-product Y^r of Y is not isomorphic as an algebraic variety to the jacobian of a smooth connected projective curve for all positive integers

$$r > M := \frac{p-2}{\frac{1}{p}\frac{2g_0}{p-1} - a}.$$

(In the case (i) we put $a = 0$.)

Proof. First, notice that the existence of κ implies that the ratio

$$\frac{2g_0}{p-1} = \frac{2\dim(Y)}{p-1}$$

is an *integer*.

Let $r > M$ be a positive integer and $X = Y^r$. Then $g := \dim(Y) = rg_0$, and the endomorphism ring $\mathrm{End}(X) = \mathrm{End}(Y^r)$ is canonically isomorphic to the matrix ring $\mathrm{Mat}_r(\mathrm{End}(Y))$ of size r over $\mathrm{End}(Y)$ with the same center as $\mathrm{End}(Y)$. In particular, the image of the *diagonal embedding*

$$\kappa_k : \mathbb{Z}[\zeta_p] \hookrightarrow \oplus_{i=1}^k \mathrm{End}(Y) \subset \mathrm{Mat}_r(\mathrm{End}(Y)), \quad u \mapsto (\kappa(u),\dots,\kappa(u)) \ \ (k \text{ times})$$

lies in the center $\mathcal{Z}_Y$ of $\mathrm{End}(Y)$. On the other hand,

$$\Omega^1(X) = \Omega^1(Y^r) = \oplus_{i=1}^r \Omega^1(Y)$$

and the linear operator

$$\delta_{X,\Omega} : \Omega^1(X) \to \Omega^1(X)$$

(which acts "diagonally" on $\Omega^1(X)$) enjoys the following properties.

Its spectrum coincides with the spectrum of $\delta_{Y,\Omega}$. In addition, if an eigenvalue γ of $\delta_{Y,\Omega}$ has multiplicity a then it has multiplicity ka, viewed as an eigenvalue of $\delta_{X,\Omega}$. Assume now that X is isomorphic to the jacobian of a smooth connected projective curve of genus g. If ζ is not an eigenvalue of $\delta_{X,\Omega}$ then it is not an eigenvalue of $\delta_{Y,\Omega}$ and therefore

$$\frac{2rg_0}{p-1} = \frac{2g}{p-1} \le p-2.$$

This implies that

$$r \le \frac{p-2}{\frac{2g_0}{p-1}} = M,$$

because in this case $a = 0$. This contradicts our assumption on r. So, ζ is an eigenvalue of $\delta_{Y,\Omega}$ and its multiplicity a satisfies the inequality

$$a < \frac{1}{p} \cdot \frac{2g_0}{p-1} = \frac{1}{p} \cdot \frac{2\dim(Y)}{p-1}.$$

Since both a and $\frac{2g_0}{p-1}$ are integers,

$$a \le \frac{1}{p} \cdot \frac{2g_0}{p-1} - \frac{1}{p}. \tag{6.2}$$

This implies that ζ is an eigenvalue of $\delta_{X,\Omega}$ and its multiplicity equals ra, which satisfies the inequality

$$ra \le r\left(\frac{1}{p} \cdot \frac{2g_0}{p-1} - \frac{1}{p}\right) = \frac{1}{p} \cdot \frac{2rg_0}{p-1} - \frac{r}{p} = \frac{1}{p} \cdot \frac{2g}{p-1} - \frac{r}{p}.$$

Taking into account that

$$\frac{1}{p}\frac{2g_0}{p-1} - a > 0, \quad r > M,$$

we get

$$ra = r \cdot \frac{1}{p}\frac{2g_0}{p-1} - r \cdot \left(\frac{1}{p}\frac{2g_0}{p-1} - a\right) < \frac{1}{p}\frac{2g_0 r}{p-1} - M\left(\frac{1}{p}\frac{2g_0}{p-1} - a\right) = \frac{1}{p}\frac{2g}{p-1} - \frac{p-2}{p}.$$

In other words, ζ is an eigenvalue of $\delta_{X,\Omega}$ with multiplicity that is strictly less than

$$\frac{1}{p}\frac{2g}{p-1} - \frac{p-2}{p},$$

which contradicts to Theorem 2.3. The obtained contradiction implies that X is not isomorphic to a jacobian. □

Example 4. *Let p be an odd prime and $n \ge 4$ an integer such that p does not divide n. We have*

$$n = ap + c; \quad a, c \in \mathbb{Z}_+; 1 \le c \le p-1; \quad 0 \le c-1 \le p-2. \tag{6.3}$$

Let $f(x) \in \mathbb{C}[x]$ be a degree n polynomial without repeated roots. Let $\mathcal{C}_{f,p}$ be the smooth projective model of the smooth plane affine curve $y^p = f(x)$. The genus g_0 of $\mathcal{C}_{f,p}$ is $(n-1)(p-1)/2$; hence

$$\frac{2g_0}{p-1} = n-1 = ap + (c-1).$$

There is an automorphism $\tilde{\delta} \in \mathrm{Aut}(\mathcal{C}_{f,p})$ of $\mathcal{C}_{f,p}$ defined by

$$(x, y) \mapsto (x, \zeta_p y).$$

Let $(J(\mathcal{C}_{f,p}),\Theta)$ *be the canonically principally polarized jacobian of* $C_{f,p}$. *By Albanese functoriality* $\tilde{\delta}$ *induces the automorphism* δ *of* $(\mathcal{J},\Theta)$, *which satisfies the* p*th cyclotomic equation. The corresponding* multiplicity function *is*

$$\mathbf{a}_{\mathcal{J}(\mathfrak{C}_{f,p}),\delta} : (-k \bmod p) \mapsto [nk/p] \ \ (1 \le k \le p-1),$$

see [20, Remark 3.7]. *In particular, in light of* (6.3),

$$\mathbf{a}_{\mathcal{J}(\mathcal{C}_{f,p}),\delta}(-1 \bmod p) = [n/p] = [(ap+c)/p] = a \tag{6.4}$$
$$= \frac{(n-1)-(c-1)}{p} = \frac{1}{p}\frac{2g_0}{p-1} - \frac{(c-1)}{p} \ge \frac{2g_0}{p-1} - \frac{p-2}{p}.$$

Let us assume that

$$c > 1,$$

i.e., p *does* not *divide* $n-1$. *Then either* ζ_p^{-1} *is not an eigenvalue of*

$$\delta_{\Omega} : \Omega^1(\mathcal{J}(\mathcal{C}_{f,p})) \to \Omega^1(\mathcal{J}(\mathcal{C}_{f,p}))$$

or it is an eigenvalue but its multiplicity, a, *is strictly less than* $\frac{1}{p}\frac{2g_0}{p-1}$. *Now it follows from Corollary 5 that if* δ *is a* central element *of* $\mathrm{End}(\mathcal{J}(\mathcal{C}_{f,p}))$ *then* $\mathcal{J}(\mathcal{C}_{f,p})^r$ *is* not *isomorphic as an algebraic variety to the jacobian of a smooth connected projective curve for all positive integers*

$$r > \frac{p-2}{\frac{1}{p}\frac{2g_0}{p-1} - a} = \frac{p-2}{\frac{1}{p}(n-1) - a} = \frac{p-2}{\frac{1}{p}(pa+c-1) - a} = \frac{p-2}{(c-1)/p} = \frac{p(p-2)}{c-1}.$$

In other words, $\mathcal{J}(\mathcal{C}_{f,p})^r$ *is not isomorphic to a jacobian (even if one ignores polarizations) if* δ *is central,* $c > 1$, *and*

$$r > \frac{p(p-2)}{c-1}.$$

Theorem 6.2. *Let* p *be an odd prime and* $n \ge 5$ *an integer. Suppose that* p *does not divide* $n(n-1)$, *i.e.,* $n = ap + c$ *where* $a, c \in \mathbb{Z}_+$, *and* $2 \le c \le p-1$. *Let* K *be a subfield of* $\mathbb{C}$ *that contains* ζ_p. *Let* $f(x) \in K[x] \subset \mathbb{C}[x]$ *be a degree* n *irreducible polynomial over* K, *whose Galois group* $\mathrm{Gal}(f/K)$ *over* K *enjoys one of the following two properties.*

- $n \ge 4$ *and* $\mathrm{Gal}(f)$ *coincides with the full symmetric group* $\mathbf{S}_n$;
- $n \ge 5$ *and* $\mathrm{Gal}(f)$ *coincides with the alternating group* $\mathbf{A}_n$.

Then $\mathcal{J}(\mathcal{C}_{f,p})^r$ *is* not *isomorphic as an algebraic variety to the jacobian of a smooth connected projective curve for all positive integers*

$$r > \frac{p(p-2)}{c-1}.$$

In particular, $\mathcal{J}(\mathcal{C}_{f,p})^r$ *is* not *isomorphic to a jacobian if* $r > p(p-2)$.

Proof. Our assumptions on n and $f(x)$ imply that the endomorphism ring $\mathrm{End}(J(\mathcal{C}_{f,p}))$ equals $\mathbb{Z}[\delta] \cong \mathbb{Z}[\zeta_p]$. Indeed, in the case $n \ge 5$, it follows from [20, Thm. 1.1] (see also corrigendum in [23, Remark 1.4] for $n = 5$); in the case $n = 4$, it follows from [22, Thm. 1.3], because $\mathbf{S}_4$ does not have a normal subgroup of index 3. In particular, the ring $\mathrm{End}(J(\mathcal{C}_{f,p}))$ is commutative and therefore δ lies in its center. Now the desired results follow readily from considerations of Example 4 if we take into account $c-1 \ge 2-1 = 1$ and therefore $p(p-2) \ge p(p-2)/(c-1)$. □

Theorem 6.3 (self-products of abelian varieties of CM type)**.** *Let* p *be an odd prime,* Y *a complex abelian variety of dimension* $(p-1)/2$ *endowed with a ring isomorphism* $\kappa : \mathbb{Z}[\zeta_p] \cong \mathrm{End}(Y)$.

If $r > (p-2)$ *is an integer then* Y^r *is not isomorphic as an algebraic variety to the jacobian of a smooth connected projective curve.*

Proof. Let us consider $\delta := \kappa(\zeta_p) \in \mathrm{Aut}(Y)$. Clearly, δ satisfies the pth cyclotomic equation in $\mathrm{End}(Y)$. On the other hand, the complex vector space $\Omega^1(Y)$ has dimension $(p-1)/2$ that is strictly less that $(p-1)$. Hence, there is a primitive pth root of unity, say, ζ that is *not* an eigenvalue of $\delta_\Omega : \Omega^1(Y) \to \Omega^1(Y)$. Now the desired result follows from Corollary 5 applied to $g_0 = (p-1)/2$ and $a = 0$. □

Example 5. *Let* $p = 3$ *and* Y *an elliptic curve with* $\mathrm{End}(Y) = \mathbb{Z}[\zeta_3]$. *It follows from Theorem 6.3 applied to* $p = 3$ *that if* $r \geq 2$ *is an integer then* Y^r *is* not *isomorphic as an algebraic variety to the jacobian of a smooth connected projective curve.* (*This assertion is well known for* $r = 2$*, see* [7].)

Acknowledgements. I am grateful to George Andrews for a very informative letter about partitions. I thank the referees for thoughtful comments that helped to improve the exposition.

References

[1] J. D. Achter & R. Pries, "The integral monodromy of hyperelliptic and trielliptic curves", *Math. Ann.* **338** (2007), no. 1, p. 187-206.

[2] G. E. Andrews & K. Eriksson, *Integer partitions*, Cambridge University Press, Cambridge, 2004, x+141 pages.

[3] M. F. Atiyah & R. Bott, "A Lefschetz fixed point formula for elliptic differential operators", *Bull. Amer. Math. Soc.* **72** (1966), p. 245-250.

[4] C. Birkenhake & H. Lange, *Complex abelian varieties*, second ed., Grundlehren der mathematischen Wissenschaften, vol. 302, Springer-Verlag, Berlin, 2004, xii+635 pages.

[5] C. H. Clemens & P. A. Griffiths, "The intermediate Jacobian of the cubic threefold", *Ann. of Math. (2)* **95** (1972), p. 281-356.

[6] P. Griffiths & J. Harris, *Principles of algebraic geometry*, Pure and Applied Mathematics, Wiley-Interscience [John Wiley & Sons], New York, 1978, xii+813 pages.

[7] T. Hayashida & M. Nishi, "Existence of curves of genus two on a product of two elliptic curves", *J. Math. Soc. Japan* **17** (1965), p. 1-16.

[8] K. Ireland & M. Rosen, *A classical introduction to modern number theory*, second ed., Graduate Texts in Mathematics, vol. 84, Springer-Verlag, New York, 1998, xiv+389 pages.

[9] S. Lang, *Algebra*, third ed., Graduate Texts in Mathematics, vol. 211, Springer-Verlag, New York, 2002, xvi+914 pages.

[10] J. Milnor, *Dynamics in one complex variable*, Friedr. Vieweg & Sohn, Braunschweig, 1999, viii+257 pages.

[11] H. L. Montgomery & R. C. Vaughan, *Multiplicative number theory. I. Classical theory*, Cambridge Studies in Advanced Mathematics, vol. 97, Cambridge University Press, Cambridge, 2007, xviii+552 pages.

[12] B. Moonen & Y. G. Zarhin, "Weil classes on abelian varieties", *J. Reine Angew. Math.* **496** (1998), p. 83-92, Erratum https://www.math.ru.nl/ bmoonen/Papers/ErratumCrelle98.pdf.

[13] D. Mumford, *Abelian varieties*, second ed., Tata Institute of Fundamental Research Studies in Mathematics, vol. 5, Tata Institute of Fundamental Research, Bombay; by Oxford University Press, London, 1974, xii+279 pages.

[14] B. Poonen & E. F. Schaefer, "Explicit descent for Jacobians of cyclic covers of the projective line", *J. Reine Angew. Math.* **488** (1997), p. 141-188.

[15] I. Reiner, *Maximal orders*, London Mathematical Society Monographs. New Series, vol. 28, The Clarendon Press, Oxford University Press, Oxford, 2003, Corrected reprint of the 1975 original, With a foreword by M. J. Taylor, xiv+395 pages.

[16] K. A. Ribet, "Galois action on division points of Abelian varieties with real multiplications", *Amer. J. Math.* **98** (1976), no. 3, p. 751-804.

[17] G. Shimura, *Abelian varieties with complex multiplication and modular functions*, Princeton Mathematical Series, vol. 46, Princeton University Press, Princeton, NJ, 1997, xvi+218 pages.

[18] A. Weil, "Zum Beweis des Torellischen Satzes", *Nachr. Akad. Wiss. Göttingen. Math.-Phys. Kl. IIa.* **1957** (1957), p. 33-53, Œuvres, vol. III, [1957a].

[19] ———, "Sur le théorème de Torelli", *Séminaire Bourbaki* (Mai 1957), no. 151.

[20] Y. G. Zarhin, "The endomorphism rings of Jacobians of cyclic covers of the projective line", *Math. Proc. Cambridge Philos. Soc.* **136** (2004), no. 2, p. 257-267.

[21] ———, "Cubic surfaces and cubic threefolds, Jacobians and intermediate Jacobians", in *Algebra, arithmetic, and geometry: in honor of Yu. I. Manin. Vol. II*, Progr. Math., vol. 270, Birkhäuser Boston, Boston, MA, 2009, p. 687-691.

[22] ———, "Endomorphism algebras of abelian varieties with special reference to superelliptic Jacobians", in *Geometry, algebra, number theory, and their information technology applications*, Springer Proc. Math. Stat., vol. 251, Springer, Cham, 2018, p. 477-528.

[23] ———, "Superelliptic jacobians and central simple representations", in *Arithmetic, Geometry, Cryptography and Coding Theory*, Contemporary Mathematics, vol. 832, American Mathematical Society, Providence, RI, 2026, To appear; arXiv:2305.12022 [math.NT].

Yuri Zarhin: Department of Mathematics, Pennsylvania State University, University Park, PA 16802, USA
E-mail: zarhin@math.psu.edu