Dedicated to Francesc Bars on the occasion of his 50th birthday

AUTOMORPHISM GROUP AND TWISTS OF A PSEUDO-FERMAT CURVE. I

ESLAM BADR

Communicated by Marian Aprodu

For an integer $d \geq 5$, let $\mathcal{C}/\mathbb{Z}$ be the scheme $x^d + y^d + xz^{d-1} = 0$. We first show that the fibres $C_{d,0} := \mathcal{C} \otimes \overline{\mathbb{Q}}$ and $C_{d,p} := \mathcal{C} \otimes \overline{\mathbb{F}}_p$ for $p \nmid d(d-1)$ are smooth plane curves having the same automorphism group. We then provide the description of the twists of $\mathcal{C} \otimes \mathbb{R}$ over $\mathbb{R}$, and these of $\mathcal{C} \otimes \mathbb{F}_p$ over $\mathbb{F}_p$. In doing so, it becomes evident that for all the twists C' of $\mathcal{C} \otimes \mathbb{Q}$, $C'(\mathbb{Q}) \neq \emptyset$, as long as d is not divisible by 3.

AMS 2020 Subject Classification: 14H37, 14H50, 14H45, 14G05, 14G17.

Key words: automorphism groups, plane curves, twists, rational points.

1. INTRODUCTION, MOTIVATION, AND MAIN RESULTS

Smooth plane curves play a central role in algebraic geometry, as they often possess rich structures and symmetries that can be studied through their automorphism groups and also their twists over a given field k. Understanding the automorphism group of a curve provides insights into the geometry of the curve, while studying twists elucidates the different ways in which a curve can be modified while preserving certain arithmetic properties.

Automorphism groups. The study of automorphism groups of smooth plane curves has connections to diverse areas of mathematics, including but not limited to representation theory, complex analysis, and number theory. For instance, the McKay correspondence in algebraic geometry relates the automorphism group of a smooth plane curve to finite groups of Lie type, providing a bridge between algebraic and geometric structures (see [13, 14, 29, 33]).

One of the key results is that any smooth curve of genus $g \neq 0, 1$ has finitely many automorphisms (see [36]). In case of smooth plane curves of degree $d \geq 4$ defined over an algebraically closed field k of characteristic $p \geq 0$, the automorphisms can be described in terms of linear transformations of the projective plane $\mathbb{P}^2_k$ (see [21, Theorem 11.29]). Moreover, the general characteristics of the structure of the automorphism groups when $p = 0$ are known

MATH. REPORTS **27(77)** (2025), *1-2*, 77–88
doi: 10.59277/mrar.2025.27.77.1.2.77

(see [19]). However, once the degree d is chosen, finding the exact list of automorphism groups becomes complex and challenging. In this direction, the classification for low degree curves $d \leq 7$ is well understood (see [1–6, 20]). In positive characteristic, i.e., when $p > 0$, the aforementioned results remain valid for all but finitely many values of p. More specifically, if the automorphism group has order divisible by p, then interesting wild things could happen (see [16, 17, 21, 22, 28]).

Twists and rational points. Let k be a perfect field, and fix $\overline{k}$ an algebraic closure of k. We use G_k for the Galois group of $\overline{k}/k$, moreover, its action is denoted by left exponentiation ${}^{\sigma}(\cdot)$ for $\sigma \in G_k$. Also, if C/k is a smooth curve over the field k, then we use $\mathrm{Aut}(C)$ for the automorphism group of the curve $C \otimes \overline{k}$.

A curve C'/k is called *a twist of* C *over* k if $C \otimes \overline{k}$ and $C \otimes \overline{k}$ are isomorphic. Computing the set $\mathrm{Twist}_k(C)$ of k-isomorphism classes of the twists of C over k can be done through the Galois cohomology group $\mathrm{H}^1(G_k, \mathrm{Aut}(C \otimes \overline{k}))$, since there is one-to-one correspondence between $\mathrm{Twist}_k(C)$ and $\mathrm{H}^1(G_k, \mathrm{Aut}(C \otimes \overline{k}))$ (see [37]). This bijection works as follows: For each $C' \in \mathrm{Twist}_k(C)$, fix an isomorphism $\Phi : C' \otimes \overline{k} \to C \otimes \overline{k}$. Then, define the corresponding 1-cocycle ξ by

$$\xi(\sigma) := \Phi \circ {}^{\tau}\Phi \text{ for } \sigma \in G_k.$$

For smooth curves of genus $g \leq 2$, the twists are well known. While the genus 0 and 1 cases go back from long ago (see [39]), the genus 2 case is due to the work of Cardona and Quer (see [10–12, 32]). All the genus $0, 1$ and 2 curves are hyperelliptic, however for genus greater than 2 almost all the curves are non-hyperelliptic. In this situation, the work of García (see [24–26]) explores the explicit computation of twists of curves. An algorithm for computing the twists of a given curve was developed assuming that its automorphism group is known. This algorithm is based on a correspondence established between the set of twists and the set of solutions of a certain Galois embedding problem. As an application, the classification of the twists of all plane quartic curves over a number field k was given. On the other hand, Meagher and Top described the twists of these curves over finite fields using techniques from the theory of Jacobian variety (see [31]). Finally, we remark that the investigation of rational points on curves can be approached through the study of twists, as the action of the twisting theory for curves can lead to new insights into the distribution and arithmetic properties of rational points (see [15, 23–27, 30, 31, 41]).

In [34], the author demonstrated that the fibres of the pseudo-Fermat quartic $C : x^4 + y^4 + xz^3 = 0$ over $\overline{\mathbb{F}}_p$ (for $p > 3$) and over $\overline{\mathbb{Q}}$ are smooth curves, each with an automorphism group of order 48, specifically $\mathrm{GAP}(48, 33)$ in GAP notation [40]. Additionally, the authors in [30] examined various arithmetic and

geometric aspects of this curve, including rational points, torsion points, and ramification points. More recently, in [9, Example 3.8], the reduction type at $p = 3$ was given, and interestingly, it was classified as the Picard curve with the smallest conductor found to date.

In this brief note, we aim to extend the studies in [9,30,34] to the smooth projective curve $C : x^d + y^d + xz^{d-1} = 0$ for $d \geq 5$. Specifically, we investigate the automorphism groups, twists, and rational points of $C \otimes \overline{\mathbb{Q}}$ and $C \otimes \overline{\mathbb{F}}_p$, respectively.

Notation 1.1. Through the paper, ζ_n is a fixed primitive nth root of unity in $\overline{k}$. A projective linear transformation acting as $x \to x$, $y \to ay$, $z \to bz$ for some $a, b \in \overline{k}^*$ is denoted by $\mathrm{diag}(1, a, b)$.

First, we prove the following theorem.

THEOREM 1.2 (Automorphism group). *The curve*

$$C_{d,p} : x^d + y^d + xz^{d-1} = 0$$

is smooth over $\overline{\mathbb{F}}_p$ if and only if $p \nmid d(d-1)$. In this case, the automorphism group is cyclic and generated by $\varphi_d := \mathrm{diag}(1, \zeta_d, \zeta_{d-1})$.

Concerning the twists over $\mathbb{R}$, we show the next theorem.

THEOREM 1.3 (Twists over $\mathbb{R}$). *There are exactly two $\mathbb{R}$-isomorphism classes of twists of the smooth plane curve $C_{d,0} : x^d + y^d + xz^{d-1} = 0$ over $\mathbb{R}$, namely the trivial twist $C_{d,0}$, and the non-trivial twist $C^{(1)}_{d,0} : x^d + y^d - xz^{d-1} = 0$ when d is odd, or $C^{(2)}_{d,0} : x^d - y^d + xz^{d-1} = 0$ when d is even.*

As a result, any twist $C'_{d,0}$ of $C_{d,0}$ over $\mathbb{R}$ admits infinitely many $\mathbb{R}$-points.

Furthermore, working over $\mathbb{F}_p$, we obtain the following results.

THEOREM 1.4 (Twists over $\mathbb{F}_p$). *Suppose that $p \nmid d(d-1)$, and let N be the number of twists of $C_{d,p}$ modulo $\mathbb{F}_p$-isomorphism.*

(i) *If $p = 1 \bmod d(d-1)$, then $N = d(d-1)$.*

(ii) *If $\gcd(p-1, d) = 1$, then $N = \gcd(p-1, d-1)$.*

(iii) *If $\gcd(p-1, d-1) = 1$, then $N = \gcd(p-1, d)$.*

(iv) *Otherwise, $N = \gcd(p-1, d-1) \cdot \gcd(p-1, d)$.*

In each case, the set of twists of $C_{d,p}$ over $\mathbb{F}_p$ are represented by

$$C^{n_0, n'_0}_{d,p} : x^d + \zeta_{p-1}^{-n_0} y^d + \zeta_{p-1}^{-n'_0} xz^{d-1} = 0,$$

for $n_0 = 0, 1, \ldots, \gcd(p-1, d) - 1$ and $n'_0 = 0, 1, \ldots, \gcd(p-1, d-1) - 1$. In particular, $(0 : 0 : 1)$ is always an $\mathbb{F}_p$-point that can be lifted to $\mathbb{Q}_p$.

2. SAME AUTOMORPHISM GROUP IN ANY CHARACTERISTIC

The full automorphism group of $C_{d,0} : x^d + y^d + xz^{d-1} = 0$ with $d \geq 5$ is known to be cyclic and is generated by $\varphi_d := \mathrm{diag}(1, \zeta_d, \zeta_{d-1})$. See Badr and Bars [2], for example.

In positive characteristic, we get the next lemma.

LEMMA 2.1. *The curve $C_{d,p}$ is a smooth plane curve of degree d if and only if the prime p does not divide $d(d-1)$.*

Proof. A projective point $(a : b : c)$ over $\overline{\mathbb{F}}_p$ is a singularity of $C_{d,p}$ if and only if $a^d + b^d + ac^{d-1} = da^{d-1} + c^{d-1} = db^{d-1} = (d-1)ac^{d-2} = 0 \bmod p$. For $p \nmid d(d-1)$, one sees that the previous system only has the trivial solution $a = b = c = 0 \bmod p$, which does not define a projective point. For $p|d-1$, we can take $a = 1, c = \zeta_{2d-2}$ and $b = 0$ in $\overline{\mathbb{F}}_p$, so that $C_{d,p}$ is singular at $(1 : 0 : \zeta_{2d-2})$. Similarly, for $p|d$, we get $(1 : \zeta_{2d} : 0)$. □

Second, we complete the proof of Theorem 1.2.

Proof of Theorem 1.2. Assuming that p is not a divisor of $d(d-1)$, we deduce by Lemma 2.1 that $C_{d,p}$ defines a smooth plane curve of genus $g = \frac{1}{2}(d-1)(d-2) \geq 6$ (so, it is non-hyperelliptic). Moreover, φ_d belongs to $G := \mathrm{Aut}(C_{d,p})$ and has order $d(d-1)$. Hence, $|G| = d(d-1) \cdot s$ for some positive integer s. Next, we aim to show that $s = 1$.

First, we know by [35] that the covering $C_{d,p} \to C_{d,p}/G$ is tamely ramified for any $p > (d-1)(d-2)+1$. The same holds for $p \leq (d-1)(d-2)+1$ such that $p \nmid s$. On the other hand, Grothendieck's study of the tame fundamental group of curves in characteristic p (see [18, XIII, §2]) tells us that tamely ramified covers can be lifted to characteristic 0. Now, lifting the curve $C_{d,p}$ and the group G to characteristic 0 guarantees us that $G = \langle\varphi\rangle$ as claimed. Indeed, if a smooth plane curve C of degree $d \geq 5$ over an algebraically closed field $\overline{k}$ of characteristic 0 admits an automorphism of order $d(d-1)$, then C is $\overline{k}$-projectively equivalent to $x^d + y^d + xz^{d-1} = 0$ and $|\mathrm{Aut}(C)| = d(d-1)$ (see [2, Theorem 1]).

Finally, we are left with the cases $p \leq (d-1)(d-2)+1$ such that p divides s but not $d(d-1)$. In this situation, let $\mathcal{R}_e$ be the finite subset of ramified points of $C_{d,p}$ that has ramification index e under the mapping $C_{d,p} \to C_{d,p}/\langle\varphi\rangle$. Then, $e = d-1, d$ or $d(d-1)$, and the quotient curve $C_{d,p}/\langle\varphi\rangle$ is the projective line $\mathbb{P}^1$. More specifically, we have that

$$\mathcal{R}_{d-1} \;=\; \big\{(\alpha : 1 : 0) \,:\, \alpha^d = -1\big\} = \mathrm{Orb}_{\langle\varphi\rangle}(\zeta_{2d} : 1 : 0),$$

$$\begin{aligned}\mathcal{R}_d &= \big\{(\beta:0:1)\,:\,\beta^{d-1}=-1\big\} = \mathrm{Orb}_{\langle\varphi\rangle}(\zeta_{2d-2}:0:1),\\ \mathcal{R}_{d(d-1)} &= \big\{(0:0:1)\big\} = \mathrm{Orb}_{\langle\varphi\rangle}(0:0:1).\end{aligned}$$

Therefore, the covering $C_{d,p} \to C_{d,p}/G$ admits at least three short orbits namely, $\mathrm{Orb}_G(\zeta_{2d}:1:0)$, $\mathrm{Orb}_G(\zeta_{2d-2}:0:1)$ and $\mathrm{Orb}_G(0:0:1)$. Denote the ramification indexes of these short orbits by e_1, e_2 and e_3, respectively. Imitating the proof of [21, Theorem 11.56], we also deduce that it cannot have more than four short orbits. Otherwise, i.e., if it admits more than four short orbits, then

$$|G| \leq 4(g-1) = 2d(d-3) < 2d(d-1),$$

contradicting the assumption that $d(d-1)p$ divides $|G|$. Furthermore, in our case, we read equation (11.18) in [21, Page 482] as

$$d-3 = 2(d-1)ps'\bigg(-2+\sum_{i=1}^{n}\frac{d_i}{e_i}\bigg),$$

for some positive integer s', where $n=3$ or 4, and $d_i \geq e_i-1$ if $p|e_i$ and $d_i = e_i-1$ otherwise. In all scenarios, we can say that $\sum_{i=1}^{n}\frac{d_i}{e_i} \geq \frac{5}{5}$, as

$$\begin{aligned}\sum_{i=1}^{n}\frac{d_i}{e_i} &\geq \sum_{i=1}^{n}\frac{e_i-1}{e_i} = \sum_{i=1}^{n}\Big(1-\frac{1}{e_i}\Big)\\ &\geq \Big(1-\frac{1}{e_1}\Big)+\Big(1-\frac{1}{e_2}\Big)+\Big(1-\frac{1}{e_3}\Big)\\ &\geq \Big(1-\frac{1}{d-1}\Big)+\Big(1-\frac{1}{d}\Big)+\Big(1-\frac{1}{d(d-1)}\Big) = 3-\frac{2}{d-1}\\ &\geq 3-\frac{2}{4} = \frac{5}{2}.\end{aligned}$$

Hence $d-3 \geq 5(d-1)ps'$, a contradiction.

Thus our claim on G follows. □

3. TWISTS OVER PERFECT FIELDS ARE DIAGONAL

As a consequence of the author's et al. work (see [8]) for smooth plane curves and its extension (see [7]) to smooth projective hypersurfaces, one can completely describe the twists over any perfect field k of characteristic $p \nmid d(d-1)$. For instance, we obtain the next results.

THEOREM 3.1 (Badr–Bars–García). *Let k be a perfect field of characteristic $p \nmid d(d-1)$ such that $3 \nmid d$ or the 3-torsion $\mathrm{Br}(k)$ [3] of the Brauer group of k is trivial. Then, any twist C'_d over k for the curve $C_{d,p}: x^d+y^d+xz^{d-1}=0$ is diagonal, in the sense that there exists a k-isomorphism $\phi: C'_{d,p} \longrightarrow C_{d,p}$ of*

the matrix form $\phi = \mathrm{diag}(1, \sqrt[d]{a},\ {}^{d-1}\sqrt{b})$ *for some* $a, b \in k^*$. *In particular,* $C'_{d,p}$ *is defined over* k *by the equation*

$$C'_{d,p} : x^d + ay^d + bxz^{d-1} = 0.$$

Moreover, any two twists $\{a, b\}$ *and* $\{a', b'\}$ *of* $C_{d,p}$ *are* k*-isomorphic if and only if* $a = a' \bmod {k^*}^d$ *and* $b = b' \bmod {k^*}^{d-1}$.

Applying Theorem 3.1 when $k = \mathbb{Q}, \mathbb{Q}_p$ and $\mathbb{R}$, we conclude that $(0 : 0 : 1)$ is always a k-point for any of the twists $C'_{d,p}$ of $C_{d,p}$ over k. Therefore, $C'_{d,p}(\mathbb{Q})$ is not empty for all twists, which implies that it is not empty for $C'_{d,p}(\mathbb{R})$ and $C'_{d,p}(\mathbb{Q}_p)$.

4. TWISTS OVER $\mathbb{R}$ AND THEIR $\mathbb{R}$-POINTS

Fix σ, the complex conjugation, as the generator of $\mathrm{Gal}(\mathbb{C}/\mathbb{R}) \simeq \mathbb{Z}/2\mathbb{Z}$. The map

$$\Phi : \mathrm{Twist}_{\mathbb{R}}(C_{d,0}) \longrightarrow \mathrm{H}^1\big(\mathbb{Z}/2\mathbb{Z}, \mathrm{Aut}(C_{d,0})\big)$$

that sends a twist $\phi : C' \to C_{d,0}$ to the class $[\xi] \in \mathrm{H}^1(\mathbb{Z}/2\mathbb{Z}, \mathrm{Aut}(C_{d,0}))$ of the 1-cocycle:

$$\xi : \sigma \mapsto \xi_\sigma := \phi \cdot {}^{\sigma}\phi^{-1} \in \mathrm{Aut}(C_{d,0})$$

is bijective. Hence, the class of ξ is uniquely determined by the class of the twist $C'/\mathbb{R}$. On the other hand, we conclude by Theorem 3.1 that we can take ϕ of the shape $\mathrm{diag}(1, \sqrt[5]{a} : \sqrt[4]{b})$ for some $a, b \in \mathbb{R}^*$. That is, $\xi_\sigma = \mathrm{diag}(1, \zeta_d^l, \zeta_{d-1}^{l'})$ for some integers $0 \le l \le d-1$ and $0 \le l' \le d-2$.

Proof of Theorem 1.3. We first claim that any of the aforementioned $d(d-1)$ many 1-cocycles is cohomologeous $\sim$ to $\xi^{(1)}$, $\xi^{(2)}$, $\xi^{(3)}$ or $\xi^{(4)}$, where

$$\begin{aligned}
\xi^{(1)} &: \sigma \mapsto \mathrm{Id},\\
\xi^{(2)} &: \sigma \mapsto \mathrm{diag}(1, 1, \zeta_{d-1}),\\
\xi^{(3)} &: \sigma \mapsto \mathrm{diag}(1, \zeta_d, 1),\\
\xi^{(4)} &: \sigma \mapsto \mathrm{diag}(1, \zeta_d, \zeta_{d-1}).
\end{aligned}$$

To see this, it suffices to show that for each cocycle associated to the pair (l, l') one finds an automorphism $\varphi_{\ell,\ell'} \in \mathrm{Aut}(C_{d,0})$ satisfying

$$\varphi_{\ell,\ell'} \cdot \xi_\sigma \cdot {}^{\sigma}\varphi_{\ell,\ell'}^{-1} \in \big\{\xi_\sigma^{(1)}, \xi_\sigma^{(2)}, \xi_\sigma^{(3)}, \xi_\sigma^{(4)}\big\}.$$

One verifies that $\varphi_{l,l'} \cdot \xi_\sigma \cdot {}^{\sigma}\varphi_{l,l'}^{-1} = \xi_\sigma \cdot \varphi_{l,l'}^2$. Accordingly, if l and l' are both even, then $\xi \sim \xi^{(1)}$ by taking $\varphi_{l,l'} = \mathrm{diag}(1, \zeta_d^{-l/2}, \zeta_{d-1}^{-l'/2})$. If l and l' are both odd, then take $\varphi_{l,l'} = \mathrm{diag}(1, \zeta_d^{-(l-1)/2}, \zeta_{d-1}^{-(l'-1)/2})$ and you get that $\xi \sim \xi^{(4)}$. If l

is even and l' is odd, then take $\varphi_{l,l'} = \mathrm{diag}(1, \zeta_d^{-l/2}, \zeta_{d-1}^{-(l'-1)/2})$ so that $\xi \sim \xi^{(2)}$. Lastly, if l is odd and l' is even, then take $\varphi_{l,l'} = \mathrm{diag}(1, \zeta_d^{-(l-1)/2}, \zeta_{d-1}^{-l'/2})$ to see that $\xi \sim \xi^{(3)}$. This shows the claim. Furthermore, we only consider $\xi_\sigma^{(i)}$ for $i = 1, 2$ when d is odd, as $\xi_\sigma^{(3)} \sim \xi_\sigma^{(1)}$ and $\xi_\sigma^{(4)} \sim \xi_\sigma^{(2)}$ through $\varphi_+ = \mathrm{diag}(1, \zeta_d^{-(d+1)/2}, 1)$. Similarly, $\xi_\sigma^{(i)}$ for $i = 1, 3$ when d is even, as $\xi_\sigma^{(2)} \sim \xi_\sigma^{(1)}$ and $\xi_\sigma^{(4)} \sim \xi_\sigma^{(3)}$ through $\varphi_- = \mathrm{diag}(1, 1, \zeta_{d-1}^{-d/2})$.

Finally, one can find an explicit isomorphism $\phi : C' \to C_{d,0}$ by solving the Galois embedding problem $\xi_\sigma^{(i)} = \phi \cdot {}^\sigma\phi^{-1}$. Moreover, there is always a solution ϕ of diagonal shape by the aid of Theorem 3.1. More explicitly,

(1) For $i = 1$, we can take $\phi = \mathrm{Id}$, so C' becomes the trivial twist:

$$C_{d,0} : x^d + y^d + xz^{d-1} = 0.$$

Assuming that d is odd, $C_{d,0}(\mathbb{R})$ would contain $(1 : -\sqrt[d]{r^{d-1}+1} : r)$ with r arbitrary in $\mathbb{R}$. Otherwise, i.e., when d is even, we have the points $(r : 1 : -\sqrt[d-1]{r^d+1})$ with $r \in \mathbb{R}$.

(2) For $i = 2$ and d odd, we can take $\phi = \mathrm{diag}(1, 1, \zeta_{2(d-1)})$, and C' becomes the non-trivial twist:

$$C_{d,0}^{(1)} : x^d + y^d - xz^{d-1} = 0.$$

In this case, $(1 : \sqrt[d]{r^{d-1}-1} : r)$ for any $r \in \mathbb{R}$ belongs to $C_{d,0}^{(1)}(\mathbb{R})$.

(3) For $i = 3$ and d even, we can take $\phi = \mathrm{diag}(1, \zeta_{2d}, 1)$, and C' becomes the non-trivial twist:

$$C_{d,0}^{(2)} : x^d - y^d + xz^{d-1} = 0.$$

Therefore, we get the points $(1 : r : \sqrt[d-1]{r^d-1})$ with $r \in \mathbb{R}$ in $C_{d,0}^{(2)}(\mathbb{R})$.

This finishes the proof of what we wanted to show in Theorem 1.3. □

5. TWISTS OVER $\mathbb{F}_p$ AND THEIR $\mathbb{F}_p$-POINTS

Throughout this section, $p \nmid d(d-1)$.

We have seen that any twist $C'_{d,0}$ of the pseudo-Fermat curve $C_{d,0}$ over $\mathbb{Q}$ is diagonal. In particular, we can always consider an isomorphism $\phi : C'_{d,0} \to C_{d,0}$ of the matrix shape $M_{a,b} = \mathrm{diag}(1, \sqrt[d]{a}, \sqrt[d-1]{b})$ for some $a, b \in \mathbb{Q}^*$. Thus $C'_{d,0}$ is defined over $\mathbb{Q}$ by the equation:

$$x^d + ay^d + bxz^{d-1} = 0.$$

Let $\mathrm{Norm}_{\mathbb{Q}}(M_{a,b})$ be the norm of $\det(M_{a,b})$ over $\mathbb{Q}$, and let $C'_{d,p}$ be the reduction of $C'_{d,0}$ over $\mathbb{F}_p$. If we further assume that $p \nmid \mathrm{Norm}_{\mathbb{Q}}(M_{a,b})$, then $C'_{d,p}$ becomes a good reduction of $C_{d,p}$, so it is a smooth plane curve of genus $g = \frac{1}{2}(d-1)(d-2)$ with cyclic automorphism group $\langle \varphi_d \rangle$ of order $d(d-1)$.

Moreover, we obtain the following proposition.

PROPOSITION 5.1. *For all primes $p > (g + \sqrt{g^2-1})^2$, the curve $C'_{d,p}$ always admits an $\mathbb{F}_p$-point that can be lifted to $\mathbb{Q}_p$.*

Proof. One reads the inequality $p > (g + \sqrt{g^2-1})^2$ as $(p+1) - 2g^2 > 2g\sqrt{g^2-1}$. Squaring both sides results in $(p+1)^2 - 4g^2 p > 0$. That is, $p+1 > 2g\sqrt{p} > g\lfloor 2\sqrt{p} \rfloor$. Under this condition, the Hasse–Weil estimate (see [38]) assures that $C'_{d,p}$ must have an $\mathbb{F}_p$-point. Furthermore, since it is a smooth point on $C'_{d,p}$, we can lift it to $\mathbb{Q}_p$ via Hensel's Lemma. □

The automorphisms of $C_{d,p}$ are precisely $\varphi_{l,l'} = \mathrm{diag}(1, \zeta_d^l, \zeta_{d-1}^{l'})$, in particular, they are uniquely determined by $l \bmod d$ and $l' \bmod d-1$. Because $\mathrm{Aut}(C_{d,p})$ is abelian, the conjugacy classes are the singleton sets $\{\varphi_{l,l'}\}$.

Now, we are going to prove Theorem 1.4.

Proof of Theorem 1.4. The Frobenius Fr acts on $\mathrm{Aut}(C_{d,p})$ as $\varphi_{l,l'} \to \varphi_{pl,pl'}$. Second, we calculate the Frobenius conjugacy classes:

$$[\varphi_{l,l'}] = \left\{ \phi \circ \varphi_{l,l'} \circ ({}^{Fr}\phi)^{-1} \,:\, \phi \in \mathrm{Aut}(C_{d,p}) \right\}$$

based on the values of $p \bmod d(d-1)$. This counts as a main ingredient for understanding the twists of $C_{d,p}$ over $\mathbb{F}_p$ (see [31, Proposition 9]). In this direction, one easily checks that $\varphi_{l,l'}$ belongs to the Frobenius conjugacy class of φ_{n_0,n'_0} if and only if there exist $0 \le n \le d$ and $0 \le n' \le d-1$ such that $\varphi_{l+n(p-1)-n_0, l'+n'(p-1)-n'_0} = \mathrm{Id}$. This is equivalent to say that

$$\begin{aligned} l + n(p-1) - n_0 &= 0 \bmod d, \\ l' + n'(p-1) - n'_0 &= 0 \bmod d-1. \end{aligned}$$

(1) In case $p = 1 \bmod d(d-1)$, all automorphisms of $C_{d,p}$ are defined over $\mathbb{F}_p$. So the action of the Galois group $\mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p) = \langle Fr \rangle$ on $\mathrm{Aut}(C_{d,p})$ is trivial. In particular, Frobenius conjugation is the same as conjugation, so there are exactly $d(d-1)$ Frobenius conjugacy classes of cardinality one each. This implies that the curve $C_{d,p}$ has exactly $d(d-1)$ twists over $\mathbb{F}_p$.

(2) If $\gcd(p-1, d) = 1$, then d must be odd, and $p-1 \,(\mathrm{mod}\, d)$ is a unit in $\mathbb{Z}/d\mathbb{Z}$. Thus, for any given value of l in $\{0, 1, \ldots, d-1\}$, we have the solution $n = n_0 - l(p-1)^{-1} \,(\mathrm{mod}\, d)$ to the first equation.

Now, if $m' := \gcd(p-1, d-1)$, then $m' \geq 2$ and it must divide $l' - n'_0$. This would allow us to simplify the second equation into

$$\frac{l'-n'_0}{m'} + n'\Big(\frac{p-1}{m'}\Big) = 0 \bmod \Big(\frac{d-1}{m'}\Big).$$

Writing $l' = m'l'_1 + n'_0$ with $l'_1 \in \{0, 1, \ldots, \frac{d-1}{m'} - 1\}$, one verifies that $n' = (\frac{n'_0 - l'_1}{m'})(\frac{p-1}{m'})^{-1}$ solves the above equation modulo $\frac{d-1}{m'}$. That is, the Frobenius conjugacy class of φ_{n_0,n'_0} has cardinality $\frac{d(d-1)}{m'}$, more precisely,

$$[\varphi_{n_0,n'_0}] = \Big\{\varphi_{l,m'l'_1+n'_0} : l \in \{0,1,\ldots,d-1\},\, l'_1 \in \Big\{0,1,\ldots,\frac{d-1}{m'}-1\Big\}\Big\}.$$

Summing up, we have exactly m'-many Frobenius conjugacy classes that are represented by φ_{0,n'_0} for $n'_0 = 0, 1, \ldots, m'-1$, where each of them has cardinality $\frac{d(d-1)}{m'}$.

(3) If $\gcd(p-1, d-1) = 1$, then d must be even, and $p - 1 \pmod{d-1}$ is a unit in $\mathbb{Z}/(d-1)\mathbb{Z}$. Thus, for any given value of l' in $\{0, 1, \ldots, d-2\}$, we have the solution $n' = n'_0 - l'(p-1)^{-1} \pmod{d-1}$ to the second equation. If we let $m := \gcd(p-1, d)$, then $m \geq 2$ and it must divide $l - n_0$. Similarly as before, we can replace the first equation with

$$\frac{l-n_0}{m} + n\Big(\frac{p-1}{m}\Big) = 0 \bmod \Big(\frac{d}{m}\Big).$$

Writing $l = ml_1 + n_0$ with $l_1 \in \{0, 1, \ldots, \frac{d}{m} - 1\}$, one obtains the solution $n = (\frac{n_0 - l_1}{m})(\frac{p-1}{m})^{-1}$ modulo $\frac{d}{m}$. Hence, the Frobenius conjugacy class of φ_{n_0,n'_0} has cardinality $\frac{d(d-1)}{m}$. More precisely,

$$[\varphi_{n_0,n'_0}] = \Big\{\varphi_{ml_1+n_0,l'} : l_1 \in \Big\{0,1,\ldots,\frac{d}{m}-1\Big\},\, l' \in \{0,1,\ldots,d-2\}\Big\}.$$

Thus, we have exactly m-many Frobenius conjugacy classes represented by $\varphi_{n_0,0}$ for $n_0 = 0, 1, \ldots, m-1$.

(4) It remains to tackle the case when $m, m' > 1$. In this situation, $m \,|\, l - n_0$ and $m' \,|\, l' - n'_0$, therefore, it suffices to deal with the system:

$$\begin{aligned} \frac{l-n_0}{m} + n\Big(\frac{p-1}{m}\Big) &= 0 \bmod \frac{d}{m}, \\ \frac{l'-n'_0}{m'} + n'\Big(\frac{p-1}{m'}\Big) &= 0 \bmod \Big(\frac{d-1}{m'}\Big). \end{aligned}$$

Writing $l = ml_1 + n_0$ with $l_1 \in \{0, 1, \ldots, \frac{d}{m} - 1\}$, and $l' = m'l'_1 + n'_0$ with $l'_1 \in \{0, 1, \ldots, \frac{d-1}{m'} - 1\}$, one sees that $n = (\frac{n_0 - l_1}{m})(\frac{p-1}{m})^{-1} \bmod \frac{d}{m}$ and $n' = (\frac{n'_0 - l'_1}{m'})(\frac{p-1}{m'})^{-1} \bmod (\frac{d-1}{m})$ is a solution to the aforementioned

system. That is, the Frobenius conjugacy class of $\varphi_{n_0,n_0'}$ has cardinality $\frac{d(d-1)}{mm'}$. More concretely,

$$[\varphi_{n_0,n_0'}]=\Big\{\varphi_{ml_1+n_0,m'l_1'+n_0'}: l_1\in\Big\{0,1,\dots,\frac{d}{m}-1\Big\}, l_1'\in\Big\{0,1,\dots,\frac{d-1}{m'}-1\Big\}\Big\}.$$

Accordingly, we have exactly mm'-many Frobenius conjugacy classes represented by $\varphi_{n_0,n_0'}$ for $n_0=0,1,\dots,m-1$ and $n_0'=0,1,\dots,m'-1$, where each of them has cardinality $\frac{d(d-1)}{mm'}$.

Finally, denoting the corresponding twists by $C_{d,p}^{n_0,n_0'}$, for $n_0=0,1,\dots,m-1$ and $n_0'=1,2,\dots,m'-1$, we can take $\phi_{n_0,n_0'}:=\mathrm{diag}(1,\zeta_{d(p-1)}^{-n_0},\zeta_{(d-1)(p-1)}^{-n_0'})$ as an explicit isomorphism $\phi_{n_0,n_0'}: C_{d,p}^{n_0,n_0'}\to C_{d,p}$ satisfying the cocycle condition $\xi^{(n_0,n_0')}(Fr)=\phi\cdots{}^{Fr}\phi^{-1}$. Here, $\xi^{(n_0,n_0')}$ is the cocycle $Fr\to\varphi_{n_0,n_0'}$. In particular, the twist $C_{d,p}^{n_0,n_0'}$ is defined over $\mathbb{F}_p$ by the equation:

$$x^d+\zeta_{p-1}^{-n_0}y^d+\zeta_{p-1}^{-n_0'}xz^{d-1}=0.$$

This completes the proof. □

Acknowledgments. The author sincerely appreciates the anonymous referees for their careful and comprehensive review of the paper. Their constructive feedback and insightful suggestions have greatly enhanced the clarity and quality of this work. I am grateful for their expertise, which has allowed me to strengthen the arguments and improve the presentation of our results.

REFERENCES

[1] E. Badr and F. Bars, *Automorphism groups of nonsingular plane curves of degree 5.* Comm. Algebra **44** (2016), *10*, 4327–4340.

[2] E. Badr and F. Bars, *Non-singular plane curves with an element of "large" order in its automorphism group.* Internat. J. Algebra Comput. **26** (2016), *2*, 399–433.

[3] E. Badr and F. Bars, *On fake ES-irreducibile components of certain strata of smooth plane sextics.* J. Algebra Appl. **24** (2025), *2*, article no. 2550048.

[4] E. Badr and F. Bars, *The stratification by automorphism groups of smooth plane sextic curves*. Ann. Mat. Pura Appl. (2025).

[5] E. Badr, A. El-guindy, and M. Kamel, *Automorphism groups and signatures of smooth septic curves*. Glasg. Math. J., Published online (2025), 1–22.

[6] E. Badr and E. García Lorenzo, *A note on the stratification by automorphisms of smooth plane curves of genus 6.* Colloq. Math. **159** (2020), *2*, 207–222.

[7] E. Badr and F. Bars, *Hypersurface model-fields of definition for smooth hypersurfaces and their twists.* Acta Arith. **194** (2020), *3*, 267–280.

[8] E. Badr, F. Bars, and E. Lorenzo Garcìa, *On twists of smooth plane curves*. Math. Comp. **88** (2019), *315*, 421–438.

[9] M. Börner, I.I. Bouw, and S. Wewers, *Picard curves with small conductor*. In: Böckle et al. (Eds.), *Algorithmic and Experimental Methods in Algebra, Geometry, and Number Theory*, pp. 97–122. Springer, Cham, 2018.

[10] G. Cardona, *Models Racionals de Corbes de Genere 2*. Thesis, 2001.

[11] G. Cardona, *On the number of curves of genus 2 over a finite field*. Finite Fields Appl. **9** (2003), *4*, 505–526.

[12] G. Cardona and J. Quer, *Curves of genus* 2 *with group of automorphisms isomorphic to* D_8 *or* D_{12}. Trans. Am. Math. Soc. **359** (2007), *6*, 2831–2849.

[13] M. Cirafici and R.J. Szabo, *Curve counting, instantons and McKay correspondences*. J. Geom. Phys. **72** (2013), 54–109.

[14] I. Dolgachev, *McKay's correspondence for cocompact discrete subgroups of* $SU(1,1)$. In: J. Harnad et al. (Eds.), *Groups and Symmetries. From Neolithic Scots to John McKay*. CRM Proceedings and Lecture Notes 47, pp. 111–133. American Mathematical Society (AMS), Providence, RI, 2009.

[15] N.D. Elkies, *The Klein quartic in number theory*. In: *The Eightfold Way*, Math. Sci. Res. Inst. Publ. 35, pp. 51–101. Cambridge Univ. Press, Cambridge, 1999.

[16] M. Giulietti and G. Korchmáros, *Algebraic curves with many automorphisms*. Adv. Math. **349** (2019), 162–211.

[17] M. Giulietti and G. Korchmáros, *A new family of maximal curves over a finite field*. Math. Ann. **343** (2009), *1*, 229–245.

[18] A. Grothendieck et al. (Eds.), *Revêtements étales et géométrie algébrique (SGA 1)*. Lecture Notes in Math. 224, Springer, Heidelberg, 1971.

[19] T. Harui, *Automorphism groups of plane curves*. Kodai Math. J. **42** (2019), *2*, 308–331.

[20] P. Henn, *Die Automorphismengruppen dar algebraischen Functionenkorper vom Geschlecht 3*. Inagural Dissertation, Heidelberg, 1976.

[21] J.W.P. Hirschfeld, G. Korchmáros, and F. Torres, *Algebraic Curves Over a Finite Field*, Vol. 20. Princeton Ser. Appl. Math., Princeton Univ. Press, Princeton, NJ, 2008.

[22] G. Korchmáros and M. Montanucci, *Ordinary algebraic curves with many automorphisms in positive characteristic*. Algebra Number Theory **13** (2019), *1*, 1–18.

[23] R. Lercier, C. Ritzenthaler, F. Rovetta, and J. Sijsling, *Parametrizing the moduli space of curves and applications to smooth plane quartics over finite fields*. LMS J. Comput. Math. **17** (2014), 128–147.

[24] E. Lorenzo García, *Arithmetic properties of non-hyperelliptic genus 3 curves*. PhD Thesis, Universitat Politecnica de Cataluna, 2014.

[25] E. Lorenzo García, *Twists of non-hyperelliptic curves*. Rev. Mat. Iberoam. **33** (2017), *1*, 169–182.

[26] E. Lorenzo García, *Twists of non-hyperelliptic curves of genus 3*. Int. J. Number Theory **14** (2018), *6*, 1785–1812.

[27] E. Lorenzo García and M. Vullers, *Counterexamples to the Hasse principle among the twists of the Klein quartic*. Indag. Math. (N.S.) **35** (2024), *4*, 638–645.

[28] S. Nakajima, *p-ranks and automorphism groups of algebraic curves.* Trans. Amer. Math. Soc. **303** (1987), *2*, 595–607.

[29] Y. Ito and M. Reid, *The McKay correspondence for finite subgroups of* $\mathrm{SL}(3,\mathbb{C})$. In: *Higher-dimensional Complex Varieties* (Trento, 1994), pp. 221–240. de Gruyter, Berlin, 1996.

[30] M.J. Klassen and E.F. Schaefer, *Arithmetic and geometry of the curve* $y^3+1=x^4$. Acta Arithm. **74** (1996), *3*, 241–257.

[31] S. Meagher and J. Top, *Twists of genus three curves over finite fields.* Finite Fields Appl. **16** (2010), *5*, 347–368.

[32] J. Quer, *Liftings of projective* 2*-dimensional Galois representations and embedding problems.* J. Algebra **171** (1995), *2*, 541–566.

[33] M. Reid, *McKay correspondence.* 1997, arXiv: 9702016v3.

[34] C. Ritzenthaler, *Automorphism group of* $C : y^3 + x^4 + 1 = 0$ *in characteristic p.* JP J. Algebra Number Theory Appl. **4** (2004), *3*, 621–623.

[35] P. Roquette, *Abschätzung der Automorphismenzahl von Funktionenkörpern bei Primzahlcharakteristik.* Math. Z. **117** (1970), 157–163.

[36] H.L. Schmid, *Über die Automorphismen eines algebraischen Funktionenkörpers von Primzahlcharakteristik.* J. Reine Angew. Math. **179** (1938), 5–15.

[37] J.-P. Serre, *Cohomologie Galoisienne*, Fifth Edition. Lecture Notes in Math. 5, Springer, Berlin, 1994.

[38] J.-P. Serre, *Sur le nombre des points rationnels d'une courbe algèbrique sur un corps fini.* C. R. Acad. Sci. Paris Sèr. I Math. **296** (1983), *9*, 397–402.

[39] J.H. Silverman, *The Aritmetic of Elliptic Curves.* Grad. Texts in Math. 106, Springer, New York, 1986.

[40] The GAP Group, GAP – Groups, Algorithms, and Programming, Version 4.4.11, 2008.

[41] M. Vullers, *Twists of the Klein quartic and counter examples to the Hasse principle.* Master's Thesis, Mathematisch Instituut, Universiteit Leiden, 2019.

Received 26 August 2024

Mathematics Department
Faculty of Science, Cairo University
Giza, Egypt
eslam@sci.cu.edu.eg
and
Mathematics and Actuarial Science Department
American University in Cairo
AUC Avenue, New Cairo, Egypt
eslammath@aucegypt.edu