TWISTS OF GENUS THREE CURVES OVER FINITE FIELDS

STEPHEN MEAGHER AND JAAP TOP

Abstract. In this article we recall how to describe the twists of a curve over a finite field and we show how to compute the number of rational points on such a twist by methods of linear algebra. We illustrate this in the case of plane quartic curves with at least 16 automorphisms. In particular we treat the twists of the Dyck-Fermat and Klein quartics. Our methods show how in special cases non-Abelian cohomology can be explicitly computed. They also show how questions which appear difficult from a function field perspective can be resolved by using the theory of the Jacobian variety.

1. Introduction

1.1. Let p be a prime, let $q := p^n$ be an integral power of p and let $\mathbb{F}_q$ be a field with q elements. A smooth projective connected curve C of field of definition $\mathbb{F}_q$ has at most finitely many rational points. From the work of Hasse-Weil with a small improvement due to Serre [Ser83b], we have that

$$q + 1 - g[2\sqrt{q}] \leq \#C(\mathbb{F}_q) \leq q + 1 + g[2\sqrt{q}]$$

where g is the geometric genus of C (i.e. the genus of $C \otimes \bar{\mathbb{F}}_q$).
There are several proofs of these bounds; we concentrate on one which is cohomological in nature. The first observation is that $C \otimes \bar{\mathbb{F}}_q$ has a Frobenius operator whose fixed points are the $\mathbb{F}_q$ rational points of $C \otimes \bar{\mathbb{F}}_q$. Associated to C is its Jacobian variety $\mathrm{Jac}(C)$. This is an Abelian variety (i.e. a projective group variety) of dimension g. From the work of Weil we know that the Frobenius endomorphism π of $\mathrm{Jac}(C)$ satisfies a degree $2g$ monic polynomial $P(X) \in \mathbb{Z}[X]$ whose roots have absolute value $\sqrt{q}$ under every embedding into $\mathbb{C}$. The trace of Frobenius $\mathrm{tr}(\pi)$ is defined to be the sum of the zeroes of $P(X)$, counted with multiplicity (so $-\mathrm{tr}(\pi)$ equals the coefficient of X^{2g-1} in $P(X)$). We then have the trace formula

$$\#C(\mathbb{F}_q) = q + 1 - \mathrm{tr}(\pi).$$

Date: March 10, 2010.

1.2. In this article we are interested in studying the Frobenius endomorphism π on $\mathrm{Jac}(C)$ for genus three curves C with many automorphisms. There are at least two basic reasons to do this, and they combine nicely to give a tractable problem. The first reason is that a curve with automorphisms also has twists. These are curves C' which are isomorphic with C over $\bar{\mathbb{F}}_q$, but not necessarily over $\mathbb{F}_q$. The second reason is that curves with many automorphisms tend to have a Jacobian variety which splits with respect to the Frobenius endomorphism. To be more concrete, all the curves C which we study have Jacobians $\mathrm{Jac}(C)$ which are isogenous to a triple product of elliptic curves. This makes it much easier to study their Frobenius endomorphisms and the Frobenius endomorphisms of their twists.

Our first objective in this article is to recall how the twists of a curve C with many automorphisms (and of arbitrary genus) are classified by 1st Galois cohomology of the automorphism group $\mathrm{Aut}(C \otimes \bar{\mathbb{F}}_q)$ of C. We then explain how to explicitly compute this Galois cohomology group in terms of representatives of certain equivalence classes in $\mathrm{Aut}(C \otimes \bar{\mathbb{F}}_q)$. Next, given a twist C' of C corresponding to an equivalence class c in $\mathrm{Aut}(C \otimes \bar{\mathbb{F}}_q)$, we discuss how to compute the Frobenius endomorphism (upto conjugacy) of $\mathrm{Jac}(C')$ in terms of c and the Frobenius endomorphism of $\mathrm{Jac}(C)$.

In the second part of this article we apply these observations to compute the twists and the Frobenius endomorphisms of Jacobians of the twists of genus three curves with a large automorphism group (of order ranging from 16 to 168). Famous examples which we treat in this article are the Klein and Dyck-Fermat quartics.

1.3. There are several reasons for this work and we now explain them. The first is that curves with many automorphisms are special and it is interesting to ask how many rational points they may or may not have. An initial hope prior to beginning this study was that the numbers of rational points on these curves might be extremal with respect to the Hasse-Weil-Serre bounds. We make remarks in this paper as to when that happens.

The second reason is that we aim to illustrate how a small amount of the theory of Jacobians can be used to answer questions which seem quite difficult from the function field perspective. In particular, modulo certain facts from the theory of Jacobian varieties, our work reduces the problem of computing the number of $\mathbb{F}_q$ points on twists to linear algebra.

A third reason is that the present work shows how non-Abelian group cohomology can be explicitly computed in certain cases.

A fourth reason is that some of the curves studied here have other interesting properties. Indeed the Klein and Dyck-Fermat curves are modular curves, and over an algebraically closed field their points correspond to elliptic curves with special properties. In fact the Klein curve is a fine moduli space and its $\mathbb{F}_q$ rational points correspond to elliptic curves over $\mathbb{F}_q$ with a level 7 structure. We note, just out of interest, that twists of modular curves occur naturally in the literature - for example, they were used by Wiles in his proof of the modularity conjecture for semi-stable curves [Rub95].

1.4. Notation.

- Throughout, k denotes a field and k^s a separable closure of k, with Galois group $G_k := \mathrm{Gal}(k^s/k)$.
- A superscripted $'$ indicates a twist; thus if C is a curve then C' is a twist of C.
- We use the tensor notation to indicate base change; thus if C is defined over k then $C \otimes k^s$ is defined over k^s.
- If V is a variety defined over k, we denote by $\mathrm{Aut}_{k^s}(V) := \mathrm{Aut}(V \otimes k^s)$ the group of automorphisms of $V \otimes k^s$.

We thank the referees of their very useful comments concerning an earlier version of this paper.

2. Twists of smooth curves

We recall the classification of twists of smooth curves in terms of the 1st Galois cohomology of the automorphism group of the curve; this case is slightly easier than the case of an arbitrary projective variety as the proofs can be given in terms of the function field of the curve. We briefly remark what is required to make the same theory work for an arbitrary quasi-projective variety. Subsections 2.2 and 2.3 follow the book [Ser94] quite closely.

2.1. Definition of twists.

Definition 1. Let V be a smooth quasi-projective variety over a field k. Let k^s be a separable closure of k. A variety V' is called a twist of V if there is an isomorphism

$$\phi : V \otimes k^s \longrightarrow V' \otimes k^s.$$

A twist V' is called trivial if there is an isomorphism

$$\phi : V \longrightarrow V'.$$

Example 2. Consider the Dyck-Fermat quartic D whose closed points in $\mathbf{P}^2$ are given by the equation

$$X^4 + Y^4 + Z^4 = 0.$$

Over $k = \mathbb{F}_{13}$, this curve has 32 points. The plane quartic D' whose projective equation is

$$X^4 + 4Y^4 - X^2Y^2 + 7Z^4 = 0$$

has 8 points, and hence these curves are not isomorphic over $\mathbb{F}_{13}$. However, over the field $\mathbb{F}_{13}(\sqrt{2})$ the map

$$(X : Y : Z) \mapsto (X + \sqrt{2}Y : X - \sqrt{2}Y : Z)$$

defines an isomorphism $D' \xrightarrow{\simeq} D$. Hence D' is a nontrivial twist of D; in fact it can be shown that it is a non-diagonal twist of D. This means that it is not isomorphic to a curve with equation

$$aX^4 + bY^4 + cZ^4 = 0$$

for $a, b, c \in \mathbb{F}_{13}^*$.

2.2. Definition of $\mathrm{H}^1(G_k, \mathrm{Aut}_{k^s}(V))$.

Definition 3. Let G be a group and let M be a group on which G acts on the left. A 1-cocycle of G with values in M is a map

$$f : G \longrightarrow M$$

such that

$$f(\sigma\tau) = f(\sigma)({}^{\sigma}f(\tau)).$$

Two cocycles f and g are called equivalent if there is an element $m \in M$ so that

$$f(\sigma)^{\sigma}m = mg(\sigma).$$

The trivial 1-cocycle is the constant map

$$f : G \longrightarrow M : \sigma \mapsto e,$$

where $e \in M$ is the unit element.

Equivalence of 1-cocycles is an equivalence relation; the set of equivalence classes of 1-cocycles is a pointed set with point represented by the trivial 1-cocycle. We write it as

$$\mathrm{H}^1(G, M).$$

Remark 4. The description for $\mathrm{H}^1(G, M)$ in terms of 1-cocycles is admittedly somewhat obscure. There are several conceptual ways of thinking about $\mathrm{H}^1(G, M)$ and we now give one. Suppose given a short exact sequence with a section s

$$\begin{tikzcd} 1 \arrow[r] & M \arrow[r] & H \arrow[r] & G \arrow[r] \arrow[l, bend left, "s"] & 1 \end{tikzcd}.$$

Set-theoretically H is a product and using this fact we can write s as

$$s(\sigma) = (f(\sigma), \sigma).$$

It is easy to check that f defines a 1-cocycle (the action of $\sigma \in G$ on M is conjugation $m \mapsto s(\sigma)ms(\sigma)^{-1}$ where M is identified with its image in H). Conversely 1-cocycles define extensions of G by M with such a section. Two 1-cocycles are equivalent if and only if their corresponding extensions are isomorphic as extensions.

Let V be an algebraic variety with field of definition k. Let $g : V \otimes k^s \longrightarrow V \otimes k^s$ be an automorphism of $V \otimes k^s$. For each $\sigma \in G_k = \mathrm{Gal}(k^s/k)$ we have a conjugated automorphism ${}^\sigma g$ defined by

$$ {}^\sigma g := (\mathrm{id}_V \otimes \sigma) \circ g \circ (\mathrm{id}_V \otimes \sigma^{-1}). $$

This formula endows $\mathrm{Aut}_{k^s}(V)$ with a left G_k action

$$ G_k \times \mathrm{Aut}_{k^s}(V) \longrightarrow \mathrm{Aut}_{k^s}(V) : \quad (\sigma, g) \mapsto {}^\sigma g. $$

The corresponding set of equivalence classes of cocycles is denoted $\mathrm{H}^1(G_k, \mathrm{Aut}_{k^s}(V))$.

2.3. **Classification of twists in terms of** $\mathrm{H}^1(G_k, \mathrm{Aut}_{k^s}(C))$**.** Let C be a smooth projective curve over a field k and let $\mathrm{Twist}(C)$ be the set of isomorphism classes of twists of C. See Proposition 5 in Chapitre III of [Ser94] for a sketch of the following proposition for all quasi-projective varieties.

Proposition 5. *There is a bijection* θ

$$ \theta : \mathrm{Twist}(C) \longrightarrow \mathrm{H}^1(G_k, \mathrm{Aut}_{k^s}(C)). $$

Proof. Let C' be a twist of C. Then there is an isomorphism

$$ \psi : C \otimes k^s \longrightarrow C' \otimes k^s. $$

An elementary calculation shows that

$$ f_\psi : \sigma \mapsto \psi^{-1} \circ {}^\sigma\psi $$

is a 1-cocycle. Given any other isomorphism

$$ \psi' : C \otimes k^s \longrightarrow C' \otimes k^s, $$

an equally elementary calculation shows that $f_{\psi'}$ is equivalent to f_ψ. We therefore define θ by

$$ \theta : C \mapsto f_\psi. $$

Let $f : G_k \longrightarrow \mathrm{Aut}_{k^s}(C)$ be a 1-cocycle. Then f defines an action of G_k on the function field $k^s(C)$ by the rule

$$ x \in k^s(C) \mapsto (\mathrm{id}_{\mathbf{P}^1} \otimes \sigma) \circ x \circ (f(\sigma^{-1}) \otimes \sigma^{-1}) $$

for every $\sigma \in G_k$. The invariants of $k^s(C)$ under this action form a function field F which is equal to $k(C')$ for some curve C' over k. By its construction C' is a twist of C. It is easy to check that this defines an inverse to θ. □

Remark 6. In the above proof we only used the fact that C was a curve in order to construct an inverse to θ. For an arbitrary quasi-projective variety the 1-cocycle can be used to make an action of the Galois group on a very ample line bundle of V following the approach taken by Mumford in GIT [GIT65]. The resulting quotient is then a twist of V. We have not given this proof as its inclusion would be more technically demanding than the object of this paper justifies.

2.4. **Calculation of** $\mathrm{H}^1(G_k, \mathrm{Aut}_{k^s}(C))$ **for** k **finite.** We now assume that k is a finite field. In this case G_k is pro-cyclic and is topologically generated by the Frobenius automorphism Fr. This fact is used in a fundamental way.

Definition 7. We call two elements $g, h \in \mathrm{Aut}_{k^s}(C)$ Frobenius conjugate if there is an element $x \in \mathrm{Aut}_{k^s}(C)$ so that

$$xg = h({}^{Fr}x).$$

It is easy to see that Frobenius conjugation defines an equivalence relation. We call an equivalence class under this equivalence relation a Frobenius conjugacy class. We thank Hendrik Lenstra for giving a proof of the following observation.

Proposition 8. *The number of Frobenius conjugacy classes is less than or equal to the number of conjugacy classes of* $\mathrm{Aut}_{k^s}(C)$.

Proof. Put $X = \mathrm{Aut}_{k^s}(C)$ and let X^h denote the elements of X fixed by h under conjugation $g \mapsto hgh^{-1}$ and let X^h_{Fr} denote the elements of X fixed by h under Frobenius conjugation $g \mapsto hg({}^{Fr}h^{-1})$. If there is a $g \in X^h_{Fr}$ then there is a bijection from $X^{({}^{Fr}h)}$ to X^h_{Fr} given by

$$g' \mapsto g \cdot g'.$$

Hence applying the Burnside Lemma (which, according to [Neu79] and [Wr81] should more appropriately be called the Cauchy-Frobenius Lemma) twice,

$$\begin{aligned} |\{\text{Frob. conj. classes of } \mathrm{Aut}_{k^s}(C)\}| &= \frac{1}{|X|}\sum_{h\in X} |X^h_{Fr}| \\ &\le \frac{1}{|X|}\sum_{h\in X} |X^h| \\ &= |\{\text{conj. classes of } \mathrm{Aut}_{k^s}(C)\}|. \end{aligned}$$

□

The next result requires the fact that G_k is pro-cyclic with topological generator Fr.

Proposition 9. *The map*

$$\mathrm{H}^1(G_k, \mathrm{Aut}_{k^s}(C)) \longrightarrow \{\text{Frobenius conjugacy classes of } \mathrm{Aut}_{k^s}(C)\}$$

given by

$$\eta : f \mapsto \textit{class of } f(Fr)$$

is a bijection.

Proof. This is a variation on an argument explained in [Ser79, Chapter XIII, §1]. To be specific, let $\alpha \in \mathrm{Aut}_{k^s}(C)$. Then a positive integer

m exist such that ${}^{Fr^m}\alpha = \alpha$. Now put $\beta := \alpha \cdot {}^{Fr}\alpha \cdot {}^{Fr^2}\alpha \cdot \ldots \cdot {}^{Fr^{m-1}}\alpha$. Let n be the order of $\beta \in \mathrm{Aut}_{k^s}(C)$. Then $\beta = {}^{Fr^m}\beta$ and

$${}^{1+Fr+\cdots+Fr^{mn-1}}\alpha = \beta \cdot {}^{Fr^m}\beta \cdot {}^{Fr^{2m}}\beta \cdot \ldots \cdot {}^{Fr^{(n-1)m}}\beta = \beta^n = \mathrm{id},$$

and hence $Fr \mapsto \alpha$ extends uniquely to a continuous cocycle $G_k \to \mathrm{Aut}_{k^s}(C)$.
Evidently every cocycle f is obtained in this way, by taking $\alpha = f(Fr)$. Two such cocycles f, g are equivalent if and only if $f(Fr)$ and $g(Fr)$ are Frobenius conjugate. □

Thus computing $\mathrm{H}^1(G_k, \mathrm{Aut}_{k^s}(C))$ is equivalent to computing the Frobenius conjugacy classes of $\mathrm{Aut}_{k^s}(C)$. Combining Propositions 5, 8 and 9 one concludes

Corollary 10. *For k finite,* $|\mathrm{Twist}(C)| =$

$$= |\{\textit{Frob. conj. classes of } \mathrm{Aut}_{k^s}(C)\}| \leq |\{\textit{conj. classes of } \mathrm{Aut}_{k^s}(C)\}|\,.$$

□

3. Jacobians and Jacobians of Twists

3.1. **Properties of the Jacobian.** Associated to a smooth projective curve C of genus g is its Jacobian variety $\mathrm{Jac}(C)$. We will use the following facts about $\mathrm{Jac}(C)$:

(a) $\mathrm{Jac}(C \otimes \bar{\mathbb{F}}_q)$ is an abelian variety of dimension g - i.e., a projective group variety - and is thus a commutative group variety and therefore has an endomorphism ring $\mathrm{End}(\mathrm{Jac}(C \otimes \bar{\mathbb{F}}_q))$ which one also denotes as $\mathrm{End}_{\bar{\mathbb{F}}_q}(\mathrm{Jac}(C))$ (see [Mil86b, p. 168, Theorem 1.1]).

(b) If ϕ is an endomorphism of $\mathrm{Jac}(C \otimes \bar{\mathbb{F}}_q)$ there is a monic polynomial $P(X)$ of degree $2g$ with coefficients in $\mathbb{Z}$ so that $P(\phi) = 0$. It is characterized by the property that for every prime number ℓ not dividing q, the polynomial $P \bmod \ell$ is the characteristic polynomial of ϕ restricted to the points of order ℓ in $\mathrm{Jac}(C \otimes \bar{\mathbb{F}}_q)$. The trace $\mathrm{tr}(\phi)$ of ϕ is defined to be the sum of zeroes of $P(X)$ (compare [Mil86a, pp. 123-125, Propositions 12.4, 12.9]). For endomorphisms ϕ and ψ we have

$$\mathrm{tr}(\phi\psi) = \mathrm{tr}(\psi\phi).$$

(c) The Jacobian is functorial in C and there is a natural isomorphism

$$\mathrm{Jac}(C \otimes \bar{\mathbb{F}}_q) = \mathrm{Jac}(C) \otimes \bar{\mathbb{F}}_q.$$

The absolute Frobenius morphism

$$fr : C \otimes \bar{\mathbb{F}}_q \longrightarrow C \otimes \bar{\mathbb{F}}_q$$

is defined by the property that its action on functions $f \in \bar{\mathbb{F}}_q(C)$ is given by $f \mapsto f^q$. It is the identity on the underlying topological space. Note that fr is not $\bar{\mathbb{F}}_q$-linear.

The relative Frobenius morphism

$$F : C \otimes \bar{\mathbb{F}}_q \longrightarrow C \otimes \bar{\mathbb{F}}_q$$

is defined on rational functions $a \otimes f \in \bar{\mathbb{F}}_q \otimes \mathbb{F}_q(C)$ by the assignment $a \otimes f \mapsto a \otimes f^q$. It induces an endomorphism

$$\pi : \mathrm{Jac}(C \otimes \bar{\mathbb{F}}_q) \longrightarrow \mathrm{Jac}(C \otimes \bar{\mathbb{F}}_q).$$

Furthermore if $Fr \in \mathrm{Gal}(\bar{\mathbb{F}}_q/\mathbb{F}_q)$ is the Frobenius automorphism then

$$\pi = \mathrm{Jac}(fr) \otimes Fr^{-1}.$$

(d) The Weil trace formula: $\#C(\mathbb{F}_q) = q+1-\mathrm{tr}(\pi)$ holds ([Mil86a, p. 143, Theorem 19.1], [Mil86b, p. 200, Theorem 11.1]).

(e) Let O be the identity element of $\mathrm{Jac}(C \otimes \bar{\mathbb{F}}_q)$ and denote by $T_O\mathrm{Jac}(C \otimes \bar{\mathbb{F}}_q)$ the tangent space at O considered as an $\bar{\mathbb{F}}_q$ vector space. Let $\Omega^1_C(C)$ be the $\bar{\mathbb{F}}_q$ vector space of regular one forms on $C \otimes \bar{\mathbb{F}}_q$. There is a canonical isomorphism

$$(T_O\mathrm{Jac}(C \otimes \bar{\mathbb{F}}_q))^* \cong \Omega^1_C(C)$$

([Mil86b, p. 171, Proposition 2.1]).

3.2. **Frobenius of a twist.** If C' is a twist of C, then given an isomorphism

$$\psi : C \otimes \bar{\mathbb{F}}_q \longrightarrow C' \otimes \bar{\mathbb{F}}_q$$

by functoriality and compatibility with change of ground field we obtain an induced isomorphism

$$\mathrm{Jac}(\psi) : \mathrm{Jac}(C') \otimes \bar{\mathbb{F}}_q \longrightarrow \mathrm{Jac}(C) \otimes \bar{\mathbb{F}}_q.$$

The reason for the reverse in the direction of the arrow is that Jac is considered as a contravariant functor. In particular, we use this induced isomorphism to identify the endomorphism rings of $\mathrm{Jac}(C \otimes \bar{\mathbb{F}}_q)$ and $\mathrm{Jac}(C' \otimes \bar{\mathbb{F}}_q)$.

Recall (Proposition 5) that the isomorphism ψ defines a 1-cocycle by the formula

$$f(\sigma) = \psi^{-1} \circ {}^{\sigma}\psi.$$

Proposition 11. *Identifying $f(\sigma)$ with its induced automorphism $\mathrm{Jac}(f(\sigma))$ on $\mathrm{Jac}(C \otimes \bar{\mathbb{F}}_q)$, one has that the Frobenius endomorphism π' of $\mathrm{Jac}(C' \otimes \bar{\mathbb{F}}_q)$ satisfies*

$$\pi' = \pi f(Fr).$$

Proof. Making the identifications explicit, the relative Frobenius endomorphism π' on $\mathrm{Jac}(C' \otimes \bar{\mathbb{F}}_q)$ corresponds to $\mathrm{Jac}(\psi) \circ \pi' \circ \mathrm{Jac}(\psi^{-1})$ on $\mathrm{Jac}(C \otimes \bar{\mathbb{F}}_q)$. On $\mathrm{Jac}(C \otimes \bar{\mathbb{F}}_q)$ we moreover have

$$\mathrm{Jac}(f(Fr)) = \mathrm{Jac}(\psi^{-1} \circ {}^{Fr}\psi) = Jac({}^{Fr}\psi) \circ \mathrm{Jac}(\psi^{-1}).$$

Observe that absolute Frobenius commutes with $\mathrm{Jac}(\psi)$, i.e. (writing here fr, fr' for the absolute Frobenius on $\mathrm{Jac}(C \otimes \bar{\mathbb{F}}_q)$ and $\mathrm{Jac}(C' \otimes \bar{\mathbb{F}}_q)$, respectively), $\mathrm{Jac}(\psi) \circ fr' = fr \circ \mathrm{Jac}(\psi)$. Using 3.1 (c) we conclude $\mathrm{Jac}(\psi) \circ \pi' \circ \mathrm{Jac}(\psi^{-1}) =$

$$\begin{aligned}
&= \mathrm{Jac}(\psi) \circ \left(fr' \otimes Fr^{-1}\right) \circ \mathrm{Jac}(\psi^{-1}) \\
&= \mathrm{Jac}(\psi) \circ \left((\mathrm{Jac}(\psi^{-1}) \circ fr \circ \mathrm{Jac}(\psi)) \otimes Fr^{-1}\right) \circ \mathrm{Jac}(\psi^{-1}) \\
&= \left(fr \otimes Fr^{-1}\right) \circ (\mathrm{id} \otimes Fr) \circ \left(\mathrm{Jac}(\psi) \otimes Fr^{-1}\right) \circ \mathrm{Jac}(\psi^{-1}) \\
&= \pi \circ \mathrm{Jac}({}^{Fr}\psi) \circ \mathrm{Jac}(\psi^{-1}) \\
&= \pi \circ \mathrm{Jac}(f(Fr))
\end{aligned}$$

and the proposition follows. □

Since we are only interested in the trace of π', by Property (b) of the preceding subsection it is enough to calculate $f(Fr)\pi$.

3.3. **The case when** $\mathrm{Jac}(C)$ **splits.** The curves of genus 3 studied in the remainder of this paper all have many automorphisms. In each case the curve considered has a characteristic 0 model and we consider only automorphisms which are defined in characteristic 0. In each case it turns out that there are automorphisms $\sigma_1, \sigma_2, \sigma_3$ so that the quotient curves C/σ_i have genus 1, so their Jacobian varieties are elliptic curves E_i.

The quotient morphisms

$$q_i : C \longrightarrow C/\sigma_i$$

induce morphisms of group varieties

$$\mathrm{Jac}(q_i) : E_i \longrightarrow \mathrm{Jac}(C).$$

In each case we study we show that the sum of these morphisms

$$\sum_i \mathrm{Jac}(q_i) : E_1 \times E_2 \times E_3 \longrightarrow \mathrm{Jac}(C)$$

has finite kernel and is surjective, i.e. it is an isogeny.

To check that $\sum_i \mathrm{Jac}(q_i)$ is an isogeny we make use of Property (e) of Subsection 3.1, namely we have a canonical isomorphism

$$(T_O \mathrm{Jac}(C))^* = \Omega^1_C(C).$$

Then $\sum \mathrm{Jac}(q_i)$ is an isogeny if and only if $\Omega^1_C(C)$ is the span of the images $q_i^* \Omega^1_{C/\sigma_i}(C/\sigma_i)$.

If $\sum_i \mathrm{Jac}(q_i)$ is an isogeny, it follows that

$$\mathrm{End}(\mathrm{Jac}(C \otimes \bar{\mathbb{F}}_q)) \otimes \mathbb{Q} \cong \mathrm{End}(E_1 \times E_2 \times E_3) \otimes \mathbb{Q}.$$

Under this identification, the Frobenius π on $\mathrm{Jac}(C \otimes \bar{\mathbb{F}}_q)$ corresponds to $\pi_1 \times \pi_2 \times \pi_3$ – the product of the Frobenius endomorphisms on the E_i. By also describing possible cocycle images $f(Fr)$ as elements of the endomorphism algebra $\mathrm{End}(E_1 \times E_2 \times E_3) \otimes \mathbb{Q}$, the problem of determining the number of $\mathbb{F}_q$ points on the twist corresponding to $f(Fr)$ is (by Proposition 11) reduced to calculating traces of certain endomorphisms of elliptic curves. We illustrate this strategy in the remaining sections of this paper.

Under the hypothesis that C is defined over the algebraic closure of $\mathbb{Q}$ we now briefly describe how to find, given $g \in \mathrm{Aut}(C \otimes \bar{\mathbb{Q}})$, the $g_{ij} \in \mathrm{Hom}(E_j, E_i) \otimes \mathbb{Q}$ such that $(g_{ij}) \in \mathrm{End}(E_1 \times E_2 \times E_3) \otimes \mathbb{Q}$ corresponds to $\mathrm{Jac}(g) \in \mathrm{End}(\mathrm{Jac}(C \otimes \bar{\mathbb{F}}_q)) \otimes \mathbb{Q} \cong \mathrm{End}(E_1 \times E_2 \times E_3) \otimes \mathbb{Q}$. First of all given $g \in \mathrm{Aut}(C \otimes \bar{\mathbb{Q}})$ we define g_{ij} as the composition

$$g_{ji}: \ E_i \xrightarrow{\mathrm{Jac}(q_i)} \mathrm{Jac}(C) \xrightarrow{\lambda_\Theta} \mathrm{Jac}(C)^t \xrightarrow{\mathrm{Jac}(q_j)^t} E_j.$$

In this composition, $\lambda_\Theta : \mathrm{Jac}(C) \longrightarrow \mathrm{Jac}(C)^t$ is the canonical principal polarisation determined by the theta divisor of $\mathrm{Jac}(C)$ ([Mil86b, p. 186 Thm. 6.6]). Observe that since $\mathrm{Jac}(C)$ is a group variety, its tangent bundle is free of rank $\dim(\mathrm{Jac}(C))$ and hence canonically isomorphic with the sheaf of differentials (by duality). Using this we deduce that g_{ji}^* (the map between differentials, induced by g_{ji}) is given by the composition

$$g_{ji}^*: \ \ \Omega^1_{E_i}(E_i) \xrightarrow{q_i^*} \Omega^1_C(C) \xrightarrow{p_j} \Omega^1_{E_j}(E_j).$$

Here p_j denotes projection. We therefore have defined an injective map by the composition

$$\mathrm{Aut}(C) \longrightarrow \bigoplus_{i,j} \mathrm{Hom}(E_i, E_j) \longrightarrow \bigoplus_{i,j} \mathrm{Hom}(\Omega^1_{E_j}(E_j), \Omega^1_{E_i}(E_i)) \ .$$

Since $\mathrm{Hom}(E_i, E_j) \otimes \bar{\mathbb{Q}} \cong \mathrm{Hom}(\Omega^1_{E_j}(E_j), \Omega^1_{E_i}(E_i)) \otimes \bar{\mathbb{Q}}$, we see that g_{ij} is uniquely determined by g_{ij}^*.

3.4. **Twists of a Jacobian.**

In some of the examples we will discuss, it is convenient to use (isogeny classes of) twists of a Jacobian variety $\mathrm{Jac}(C)$.

In particular, suppose the curve C and the elliptic curves E_j are defined over k, and an isogeny $\mathrm{Jac}(C) \to E_1 \times E_2 \times E_3$ exists over some extension of k. This means that $\mathrm{Jac}(C)$ is isogenous to a twist of the abelian variety $E_1 \times E_2 \times E_3$. Just as in the case of curves, this twist corresponds to an element in $\mathrm{H}^1(G_k, \mathrm{Aut}_{k^s}(E_1 \times E_2 \times E_3))$. In particular, for $k = \mathbb{F}_q$ and $\pi \in \mathrm{End}(E_1 \times E_2 \times E_3)$ the Frobenius endomorphism and a cocycle given by $Fr \mapsto \sigma \in \mathrm{Aut}(E_1 \times E_2 \times E_3)$, the Frobenius endomorphism on $\mathrm{Jac}(C)$ can be identified with $\pi\sigma \in \mathrm{End}(E_1 \times E_2 \times E_3)$.

4. Plane quartics with 24 automorphisms

The plane quartic curves C_a given as

$$C_a \;:\; x^4+y^4+z^4=(a+1)(x^2y^2+y^2z^2+z^2x^2)$$

were introduced by E. Ciani in 1899 [Ci99]; see also [Ed45]. More recently, they appear in [Ver83], [Ser85, Se.72], [Top89], [BST97] and in [AT02]. We consider C_a over $\mathbb{F}_q$ with q odd, and start by listing some basic facts concerning these curves.

(1) C_a is a nonsingular (hence, genus 3) curve if and only if $a\notin\{-3,0,1\}$.

(2) $\mathrm{Aut}(C_a)$ contains the automorphisms

$$\varphi \;:\; (x:y:z)\mapsto(z:x:y)$$

and

$$\psi \;:\; (x:y:z)\mapsto(-y:x:z).$$

The group G generated by φ and ψ is isomorphic to the symmetric group S_4 of order 24. An explicit isomorphism is $\varphi\mapsto(1\,2\,3)$, $\psi\mapsto(1\,3\,4\,2)$, as may be verified by considering the action of G on the four points $(1:\pm1:\pm1)\in\mathbb{P}^2$. In fact, this defines the projective representation of S_4 arising from a well-known irreducible three dimensional representation: S_4 is the group of rotations of the cube with vertices $(\pm1,\pm1,\pm1)$.

(3) If C_a is nonsingular and $a\neq-1$ and $a^2-a+16\neq0$, then $\mathrm{Aut}(C_a)=\mathrm{Aut}(C_a\otimes\bar{\mathbb{F}}_q)=G\cong S_4$.

(4) For $a=-1$, the curve has equation $x^4+y^4+z^4=0$. It is called *Dyck's quartic* after W. Dyck, who studied the curve in 1880 [Dy80]; also the name *Fermat quartic* frequently appears in the literature. In any characteristic ≥ 5, its automorphism group has precisely 96 elements. We call it the Dyck-Fermat curve, and study this case in more detail in Section 7. In characteristic 3, the automorphism group is (clearly) the group of matrices over $\mathbb{F}_9$ preserving the quadratic form $x\cdot x^3+y\cdot y^3+z\cdot z^3$, which is a simple group of order 6048.

(5) For $a^2-a+16=0$, the curve C_a is singular in characteristic 7. F. Klein (compare [Kl79, § 4] and [Top89, p. 43]) proved that this curve is isomorphic to the one given by $x^3y+y^3z+z^3x=0$ (his proof is over $\mathbb{C}$, but in fact it is valid in any characteristic $\neq 2$). The latter curve is called the *Klein curve*; its automorphism group over an algebraically closed field of characteristic $\neq 2,\neq 3,\neq 7$ is simple of order 168. In characteristic 3, the curve is a twist of the Dyck-Fermat quartic, as can be verified by comparing the ternary quadratic forms $x\cdot x^3+y\cdot y^3+z\cdot z^3$ and $x\cdot z^3+y\cdot x^3+z\cdot y^3$. In particular, for the values a considered here and odd characteristic $\neq 7$, the group $\mathrm{Aut}(C_a\otimes\bar{\mathbb{F}}_q)$ is

simple, of order 168 in characteristic $\neq 3$ and of order 6048 in characteristic 3. We will study the Klein curve in Section 8.

(6) For $a \neq 0, 1, -3$ consider the elliptic curve E_a given by

$$E_a \ : \ (a+3)y^2 = x(x-1)(x-a).$$

Define the morphism $\mu \ : \ C_a \to E_a$ by $\mu(x:y:1) :=$

$$\left(\frac{(a-1)x^4+(2a+2)x^2+a-1}{4x^2}, \frac{(a-1)(x^4-1)(2y^2-(a+1)x^2-a-1)}{8(a+3)x^3}\right).$$

Then

$$\mathrm{Jac}(\mu) + \mathrm{Jac}(\mu\varphi) + \mathrm{Jac}(\mu\varphi^2) : E_a \times E_a \times E_a \longrightarrow \mathrm{Jac}(C_a)$$

defines an isogeny, as can be verified by the method described in § 3.3 above. In particular, let π_3, π_1 denote the Frobenius endomorphism on $\mathrm{Jac}(C_a)$ and on E_a, respectively, then $\mathrm{tr}(\pi_3) = 3\mathrm{tr}(\pi_1)$. By 3.1(d), this implies

$$|C_a(\mathbb{F}_q)| = 3\,|E_a(\mathbb{F}_q)| - 2q - 2.$$

We now assume C_a is nonsingular and $a \neq -1$ and $a^2 - a + 16 \neq 0$, which implies $\mathrm{Aut}(C_a \otimes \bar{\mathbb{F}}_q) \cong S_4$. Note that all automorphisms are defined over $\mathbb{F}_q$, i.e., the Galois action on $\mathrm{Aut}(C_a \otimes \bar{\mathbb{F}}_q)$ is trivial. As a consequence, Frobenius conjugation is the same as conjugation, so one concludes that the twists of C_a are described by the conjugacy classes in $\mathrm{Aut}(C_a) \cong S_4$. There are precisely 5 such classes, corresponding to the cycle types in S_4, and given in the following table.

cycle type	generator
trivial	*id*
2-cycles	$\varphi\psi\varphi$
3-cycles	φ
4-cycles	ψ
two disjoint 2-cycles	ψ^2

As explained in 3.2, the Frobenius endomorphism on the Jacobian variety of a twist corresponding to $\sigma \in \mathrm{Aut}(C_a)$ is conjugate to a product $\sigma\pi$, which we consider in $\mathrm{End}(E_a \times E_a \times E_a) \otimes \mathbb{Q}$. To find these products, we need the endomorphisms of E_a^3 induced by φ and by ψ. These are determined by the action on the cotangent space at the origin of E_a^3 (or of $\mathrm{Jac}(C_a)$), which is a direct sum of three copies of the cotangent space at the origin of E_a, and hence by the action on the regular one forms on C_a. Namely, these one forms are spanned by the pull-back $\mu^*\omega$ for ω an invariant one form on E_a, and $\varphi^*\mu^*\omega$ and $(\varphi^2)^*\mu^*\omega$. Alternatively we may use the method described at the end of 3.3. From this, it is easily verified that (the conjugacy class of) φ induces the endomorphism (up to conjugation) $A_\varphi := \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$, and ψ induces $A_\psi := \begin{pmatrix} 0 & -1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$.

Denoting the Frobenius on E_a by π_1, the Frobinius endomorphism on E_a^3 equals π_1 times the identity matrix. Multiplying the appropriate matrices, this implies the following result.

Proposition 12. *Suppose q is odd and $a \in \mathbb{F}_q$ satisfies $a \notin \{-3, -1, 0, 1\}$ and $a^2 - a + 16 \neq 0$. There exist precisely 5 twists of C_a over $\mathbb{F}_q$, corresponding to the conjugacy classes in $\mathrm{Aut}(C_a) \cong S_4$. The trace of Frobenius on their Jacobians and their number of points over $\mathbb{F}_q$ are given in the following table.*

conjugacy class	*trace of Frobenius*	*number of points*
trivial	$3\mathrm{tr}(\pi_1)$	$3\,\lvert E_a(\mathbb{F}_q)\rvert - 2q - 2$
2-*cycles*	$-\mathrm{tr}(\pi_1)$	$-\lvert E_a(\mathbb{F}_q)\rvert + 2q + 2$
3-*cycles*	0	$q + 1$
4-*cycles*	$\mathrm{tr}(\pi_1)$	$\lvert E_a(\mathbb{F}_q)\rvert$
two disjoint 2-*cycles*	$-\mathrm{tr}(\pi_1)$	$-\lvert E_a(\mathbb{F}_q)\rvert + 2q + 2$

Remark 13. The table shows that a nontrivial twist of C_a over $\mathbb{F}_q$ does not reach the Hasse-Weil bound. Moreover, C_a over $\mathbb{F}_q$ attains this bound if and only if $E_a/\mathbb{F}_q$ does. Examples where this happens may be found in [AT02].

5. Quartics with 16 automorphisms

In this section we work over $\mathbb{F}_q$ with q odd, and consider plane quartics C_a given by

$$C_a \ : \ x^4 + y^4 + z^4 + 2ax^2y^2 = 0.$$

This defines a regular quartic curve if and only if $a \neq \pm 1$. The automorphisms

$$\sigma(x : y : z) := (y : x : z)$$

and

$$\lambda(x : y : z) := (x : y : iz)$$

(for a primitive fourth root of unity i) and

$$\mu(x : y : z) := (-x : y : z)$$

generate a group G of order 16. The center of G is the cyclic group of order 4 generated by λ.

In case $a = 0$, the curve equals the Dyck-Fermat curve which will be studied in Section 7 below. The case $a^2 + 3 = 0$ is also special, as we

will discuss in Section 6. In all remaining cases, i.e. $a \neq \pm 1, 0$ and $a^2+3 \neq 0$, a calculation shows that in fact $\mathrm{Aut}(C_a \otimes \bar{\mathbb{F}}_q) = G$.
The action of $G_{\mathbb{F}_q} = \mathrm{Gal}(\bar{\mathbb{F}}_q/\mathbb{F}_q)$ on G is trivial in case $q \equiv 1 \bmod 4$. For $q \equiv 3 \bmod 4$, the Frobenius automorphism Fr fixes σ and μ, while ${}^{Fr}\lambda = \lambda^{-1}$. With this information it is straightforward to calculate $\mathrm{H}^1(G_{\mathbb{F}_q}, G)$. For $q \equiv 1 \bmod 4$, this equals the set of conjugacy classes in G. There are 10 conjugacy classes, represented by the following elements:

$$\mathrm{id},\ \lambda,\ \lambda^2,\ \lambda^3,\ \mu,\ \sigma,\ \mu\sigma,\ \mu\lambda,\ \sigma\lambda,\ \mu\sigma\lambda.$$

So if $q \equiv 1 \bmod 4$ then C_a has precisely 10 twists over $\mathbb{F}_q$.
For $q \equiv 3 \bmod 4$, there are 8 Frobenius conjugacy classes. They are represented by

$$\mathrm{id},\ \lambda,\ \mu,\ \sigma,\ \mu\sigma,\ \mu\lambda,\ \sigma\lambda,\ \mu\sigma\lambda,$$

respectively. So $\mathrm{H}^1(G_{\mathbb{F}_q}, G)$ consists of 8 elements and C_a has exactly 8 twists over $\mathbb{F}_q$.
To count the number of points on C_a and its twists, we introduce the elliptic curves E_a and $\tilde{E}_a$, given as

$$E_a :\ y^2 = x^3 - (a^2-1)x$$

resp.

$$\tilde{E}_a :\ y^2 = x^3 - 2ax^2 + x.$$

There is a morphism $\varphi :\ C_a \to E_a$, defined by

$$\varphi(x:y:1) := \left((a^2-1)x^2, (a^2-1)(y^2+ax^2)x\right).$$

Similarly one has a morphism $\psi :\ C_a \to \tilde{E}_a$ given by

$$\psi(x:y:1) := \left(-\frac{x^2}{y^2}, \frac{x}{y^3}\right).$$

Again by the method described in § 3.3 it follows that

$$\mathrm{Jac}(\varphi) + \mathrm{Jac}(\varphi\sigma) + \mathrm{Jac}(\psi) :\ E_a \times E_a \times \tilde{E}_a \to \mathrm{Jac}(C_a)$$

defines an isogeny. Using this to identify the rings $\mathrm{End}_{\bar{\mathbb{F}}_q}(\mathrm{Jac}(C_a)) \otimes \mathbb{Q}$ and $\mathrm{End}_{\bar{\mathbb{F}}_q}(E_a \times E_a \times \tilde{E}_a) \otimes \mathbb{Q}$, this reduces the problem of counting points on twists to that of describing $\mathrm{Jac}(\lambda)$ and $\mathrm{Jac}(\sigma)$ and $\mathrm{Jac}(\mu)$ in terms of the latter ring. The curve $E_a \otimes \bar{\mathbb{F}}_q$ admits an automorphism ι of order 4, namely $\iota(x,y) := (-x, iy)$.
As before, write elements of $\mathrm{End}_{\bar{\mathbb{F}}_q}(E_a \times E_a \times \tilde{E}_a) \otimes \mathbb{Q}$ as 3×3 matrices, where the i,j-th entry denotes (up to extending scalars to $\mathbb{Q}$) a homomorphism from the j-th to the i-th elliptic curve.

With these notations, it is readily verified that Jac(λ) corresponds to $A_\lambda := \begin{pmatrix} \iota & 0 & 0 \\ 0 & \iota & 0 \\ 0 & 0 & -1 \end{pmatrix}$. Similarly, μ yields $A_\mu := \begin{pmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix}$ and for σ we obtain $A_\sigma := \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$.

Denoting Frobenius on E_a and $\tilde{E}_a$ by π resp. $\tilde{\pi}$, the Frobenius on $E_a \times E_a \times \tilde{E}_a$ is given as $\begin{pmatrix} \pi & 0 & 0 \\ 0 & \pi & 0 \\ 0 & 0 & \tilde{\pi} \end{pmatrix}$. As before, counting points on twists now boils down to considering the appropriate products of matrices. We summarize the discussion in this section as follows.

Proposition 14. *Let $\mathbb{F}_q$ be a field of odd cardinality q and suppose $a \in \mathbb{F}_q$ satisfies $a \neq \pm 1$, $a \neq 0$, and $a^2 \neq -3$.*
Then $C_a : \ x^4 + y^4 + z^4 + 2ax^2y^2 = 0$ defines a smooth plane quartic curve, with automorphism group (over $\bar{\mathbb{F}}_q$) the group G of order 16.
In case $q \equiv 1 \bmod 4$, there are precisely 10 *twists of C_a over $\mathbb{F}_q$. They correspond to cocycles Fr $\mapsto \alpha$ with $\alpha \in G$ as given in the following table. The number of rational points over $\mathbb{F}_q$ on these twists is also given in the table, in terms of the Frobenius endomorphisms $\pi, \tilde{\pi}$ of the elliptic curves given by $y^2 = x^3 - (a^2 - 1)x$ and $y^2 = x^3 - 2ax^2 + x$, respectively.*

cocycles	*number of points*	*cocycles*	*number of points*
trivial	$q+1-2\mathrm{tr}(\pi)-\mathrm{tr}(\tilde{\pi})$	σ	$q+1-\mathrm{tr}(\tilde{\pi})$
λ	$q+1-2\mathrm{tr}(\iota\pi)+\mathrm{tr}(\tilde{\pi})$	$\mu\sigma$	$q+1+\mathrm{tr}(\tilde{\pi})$
λ^2	$q+1+2\mathrm{tr}(\pi)-\mathrm{tr}(\tilde{\pi})$	$\mu\lambda$	$q+1-\mathrm{tr}(\tilde{\pi})$
λ^3	$q+1+2\mathrm{tr}(\iota\pi)+\mathrm{tr}(\tilde{\pi})$	$\sigma\lambda$	$q+1+\mathrm{tr}(\tilde{\pi})$
μ	$q+1+\mathrm{tr}(\tilde{\pi})$	$\mu\sigma\lambda$	$q+1-\mathrm{tr}(\tilde{\pi})$

In case $q \equiv 3 \bmod 4$, there are precisely 8 *twists. With their number of rational points, they are given in the next table.*

cocycles	*number of points*	*cocycles*	*number of points*
trivial	$q+1-\mathrm{tr}(\tilde{\pi})$	$\mu\sigma$	$q+1+\mathrm{tr}(\tilde{\pi})$
λ	$q+1+\mathrm{tr}(\tilde{\pi})$	$\mu\lambda$	$q+1-\mathrm{tr}(\tilde{\pi})$
μ	$q+1+\mathrm{tr}(\tilde{\pi})$	$\sigma\lambda$	$q+1+\mathrm{tr}(\tilde{\pi})$
σ	$q+1-\mathrm{tr}(\tilde{\pi})$	$\mu\sigma\lambda$	$q+1-\mathrm{tr}(\tilde{\pi})$

Remark 15. The fact that the last table contains no contributions from the curve E_a, follows from the observation that $q \equiv 3 \bmod 4$ implies that E_a is supersingular, and $\pi\iota = -\iota\pi$ so $\mathrm{tr}(\pi) = \mathrm{tr}(\iota\pi) = 0$. The term $\mathrm{tr}(\iota\pi)$ appearing in the first table is in fact the trace of Frobenius on a quartic twist of E_a over $\mathbb{F}_q$.

Remark 16. The tables in Proposition 14 show that if a twist of C_a over $\mathbb{F}_q$ reaches the Hasse-Weil bound, then $q \equiv 1 \bmod 4$ and the twist

corresponds to a cocycle defined by $Fr \mapsto \lambda^n$ for some n. Moreover, one obtains the following necessary and sufficient condition for such a twist to reach the Hasse-Weil upper bound: either $\tilde{E}_a/\mathbb{F}_q$ attains the Hasse-Weil upper bound and is isogenous to E_a or its quadratic twist, or $\tilde{E}_a/\mathbb{F}_q$ attains the Hasse-Weil lower bound and is isogenous to a bi-quadratic twist of E_a.
To obtain examples of this, take $a = 3$. In this case $\mathrm{End}_{\overline{\mathbb{F}}_q}(\tilde{E}_a)$ contains the ring $\mathbb{Z}[2i]$. So if $p > 3$ is a prime number $p \equiv 3 \bmod 4$ and $q = p^{2m}$ then $|E_a(\mathbb{F}_q)| = \left|\tilde{E}_a(\mathbb{F}_q)\right| = q + 1 - 2(-p)^m$. Hence for all odd m, the curve C_a over $\mathbb{F}_q$ attains the Hasse-Weil upper bound. For even m no twist of C_a attains the Hasse-Weil upper bound: in this case Frobenius on a bi-quadratic twist of E_a is given by $\pm p^m \iota$, so has trace 0 while Frobenius on $\tilde{E}_a$ has trace $2p^m$.

6. The quartic with 48 automorphisms

In his book [Ka95] published in 1895, S. Kantor describes on p. 86 (Theorem 90) a plane quartic curve which he claims to have exactly 72 automorphisms. This is corrected two years later by A. Wiman [Wi97, p. 226], who calculates the automorphism group to be of order 48.
An equation for the curve C in question is

$$C: \;\; y^3z + z^4 = x^4.$$

In every characteristic $\neq 2, \neq 3$, this defines a nonsingular curve of genus 3. A nice and recent paper on the arithmetic and geometry of C is [KS96]. In particular, this paper gives (Prop. 2.1) the elements of $\mathrm{Aut}_{k^s}(C)$ and describes an explicit isomorphism (defined over a field containing a zero of the polynomial $x^8 - 18x^4 - 27$) between C and the curve given by

$$x^4 + y^4 + z^4 + 2\sqrt{-3}x^2y^2 = 0.$$

Hence C is (a twist of) a specialization of the family C_a studied in Section 5. The description of C as a special curve in the family C_a was already known to E. Ciani (compare p. 420 of the expository paper [CW10]).
We briefly recall such an explicit isomorphism. Let ζ be a primitive 12th root of unity. Then $2\zeta^2 - 1$ is a square root of -3, and we have the curve

$$C_{2\zeta^2-1} \;:\; -z^4 = x^4 + (4\zeta^2 - 2)x^2y^2 + y^4.$$

Now take variables ξ, η defined by $x = (1 - \zeta^3)\xi + (\zeta^3 + \zeta^2 - \zeta - 1)\eta$ and $y = \eta - (\zeta^3 - 2\zeta - 1)\xi$. One has $x^4 + (4\zeta^2 - 2)x^2y^2 + y^4 = -16(2\zeta^3 - 4\zeta - 3)(\xi^4 + \xi\eta^3)$, so this yields the new equation

$$z^4 = 16(2\zeta^3 - 4\zeta - 3)(\xi^4 + \xi\eta^3).$$

Note that $2\zeta^3-4\zeta-3=-3\pm2\sqrt{3}$. Using $z_n:=2\gamma z$ in which γ satisfies $\gamma^4=2\zeta^3-4\zeta-3$, one obtains $z_n^4=\xi^4+\xi\eta^3$ which is the equation of the curve C.

Next we present the elements of $\mathrm{Aut}_{k^s}(C)$ in a convenient form. Put

$$\alpha_{n,m}:=\begin{pmatrix}\zeta^{3n}&0&0\\0&\zeta^{4m}&0\\0&0&1\end{pmatrix},\quad \beta_{n,m,\ell}:=\begin{pmatrix}(1+2\zeta^4)\zeta^{3n}&0&0\\0&-\zeta^{4m+4\ell}&2\zeta^{4m}\\0&\zeta^{4\ell}&1\end{pmatrix}.$$

These matrices are uniquely determined by $n \bmod 4$, $m \bmod 3$ and $\ell \bmod 3$. Hence we have $12+36=48$ matrices here. They form a subgroup G of $\mathrm{Aut}_{k^s}(\mathbb{P}^2)$ sending the curve C to itself, and in fact $\mathrm{Aut}_{k^s}(C)=G$. The following table lists the conjugacy classes in G and the order of the elements in each conjugacy class.

class	order	class	order
$\alpha_{0,0}$	1	$\{\alpha_{0,1},\ \beta_{2,1,0},\ \beta_{2,2,2},\ \beta_{2,0,1}\}$	3
$\alpha_{2,0}$	2	$\{\alpha_{1,1},\ \beta_{3,1,0},\ \beta_{3,2,2},\ \beta_{3,0,1}\}$	12
$\alpha_{1,0}$	4	$\{\alpha_{2,1},\ \beta_{0,1,0},\ \beta_{0,2,2},\ \beta_{0,0,1}\}$	6
$\alpha_{3,0}$	4	$\{\alpha_{3,1},\ \beta_{1,1,0},\ \beta_{1,2,2},\ \beta_{1,0,1}\}$	12
$\{\alpha_{0,2},\ \beta_{0,1,1},\ \beta_{0,2,0},\ \beta_{0,0,2}\}$	3	$\{\alpha_{1,2},\ \beta_{1,1,1},\ \beta_{1,2,0},\ \beta_{1,0,2}\}$	12
$\{\alpha_{2,2},\ \beta_{2,1,1},\ \beta_{2,2,0},\ \beta_{2,0,2}\}$	6	$\{\alpha_{3,2},\ \beta_{3,1,1},\ \beta_{3,2,0},\ \beta_{3,0,2}\}$	12
$\left\{\begin{array}{l}\beta_{0,0,0},\ \beta_{0,1,2},\ \beta_{0,2,1}\\ \beta_{2,0,0},\ \beta_{2,1,2},\ \beta_{2,2,1}\end{array}\right\}$	4	$\left\{\begin{array}{l}\beta_{1,0,0},\ \beta_{1,1,2},\ \beta_{1,2,1}\\ \beta_{3,0,0},\ \beta_{3,1,2},\ \beta_{3,2,1}\end{array}\right\}$	2

Working over $\mathbb{F}_q$, the Frobenius action on G is completely determined by $\zeta\mapsto\zeta^q$. So Frobenius acts as

$$\alpha_{n,m}\mapsto\alpha_{qn,qm}\ ;\ \beta_{n,m,\ell}\mapsto\begin{cases}\beta_{qn,qm,q\ell} & \text{if } q\equiv1 \bmod 3;\\ \beta_{2+qn,qm,q\ell} & \text{otherwise.}\end{cases}$$

With this information it is straightforward to calculate the Frobenius conjugacy classes. They depend on the possible values of $q \bmod 12$.

(1) In case $q\equiv1 \bmod 12$ Frobenius acts trivially, so one finds the 14 conjugacy classes presented above. In particular, the curve C has precisely 14 twists over $\mathbb{F}_q$.

(2) In case $q\equiv5 \bmod 12$ there are 6 Frobenius conjugacy classes. The table below lists for each of them a representing element and the number of elements in the class.

class of:	$\alpha_{0,0}$	$\alpha_{3,0}$	$\beta_{0,1,0}$	$\beta_{1,1,0}$	$\beta_{2,1,0}$	$\beta_{3,1,0}$
cardinality:	12	12	6	6	6	6

Hence for $q\equiv5 \bmod 12$, the curve C has precisely 6 twists over $\mathbb{F}_q$.

(3) In case $q\equiv7 \bmod 12$ there are 8 Frobenius conjugacy classes. The table below lists for each of them a representing element and the number of elements in the class.

class of:	$\alpha_{0,0}$	$\alpha_{1,0}$	$\alpha_{0,1}$	$\alpha_{0,2}$	$\alpha_{1,1}$	$\alpha_{1,2}$	$\beta_{0,0,0}$	$\beta_{1,0,0}$
cardinality:	2	2	8	8	8	8	6	6

Hence for $q \equiv 7 \bmod 12$, the curve C has precisely 8 twists over $\mathbb{F}_q$.

(4) Finally, in case $q \equiv 11 \bmod 12$ there are 4 Frobenius conjugacy classes, each containing 12 elements. These classes are represented by

$$\alpha_{0,0},\ \alpha_{1,0},\ \beta_{0,1,2},\ \beta_{1,1,0},$$

respectively. Hence for $q \equiv 11 \bmod 12$, the curve C has precisely 4 twists over $\mathbb{F}_q$.

To determine the number of points on twists of C over $\mathbb{F}_q$, recall that over some extension field, C can be given as the special case $a^2 = -3$ of the curves C_a studied in Section 5. In particular, the elliptic curve

$$E\ :\ y^2 = x^3 + 4x$$

yields two isogeny factors of $\mathrm{Jac}(C)$. The other elliptic curve appearing in $\mathrm{Jac}(C)$ is given by $y^2 = x^3 \mp 2\sqrt{-3}x^2 + x$. Over an extension containing a solution of $u^2 = \pm\sqrt{-3}$, this curve is isomorphic to the one given by $y^2 = x^3 + 6x^2 - 3x$, which in turn is 2-isogenous to

$$\tilde{E}\ :\ y^2 = x^3 + 1.$$

Consequently, $\mathrm{Jac}(C)$ is (over some extension) isogenous to

$$A := E \times E \times \tilde{E}.$$

In particular, A is over $\mathbb{F}_q$ isogenous to a twist of $\mathrm{Jac}(C)$. This implies that $\alpha \in \mathrm{Aut}_{\overline{\mathbb{F}}_q}(A)$ exists such that the Frobenius endomorphism on $\mathrm{Jac}(C)$ can (up to conjugation) be written as $\pi\alpha$, for π the Frobenius in $\mathrm{End}(A)$.

Note that an explicit morphism $C \to \tilde{E}$ can be found without the above reasoning, by simply considering the equations involved:

$$(x : y : 1) \mapsto (y, x^2)\ :\qquad C \to \tilde{E}$$

defines such a map.

We now discuss the various possibilities for q case by case. In doing so, we focus on the question whether a twist exists over $\mathbb{F}_q$ which is maximal, i.e., the number of points over $\mathbb{F}_q$ attains the Hasse-Weil-Serre upperbound $q + 1 + 3\left\lfloor 2\sqrt{q}\right\rfloor$.

In case $q \equiv 11 \bmod 12$, both E and $\tilde{E}$ are supersingular over $\mathbb{F}_q$ and moreover q is not a square. This implies that the ring of endomorphisms defined over $\mathbb{F}_q$ of E (and of $\tilde{E}$) is $\mathbb{Z}[\sqrt{-p}]$ for $p = \mathrm{char}\,\mathbb{F}_q$. In particular this means that E and $\tilde{E}$ are isogenous over $\mathbb{F}_q$, and the ring of endomorphisms of A defined over $\mathbb{F}_q$, tensored with $\mathbb{Q}$ equals $M_3(\mathbb{Q}(\sqrt{-p}))$. The (conjugacy class of) Frobenius in this ring is given by $\sqrt{-q}\cdot\mathrm{id}$, and from this it follows that on each of the four twists C' of C over $\mathbb{F}_q$, the trace of Frobenius equals 0 and therefore $|C'(\mathbb{F}_q)| = q+1$.

In case $q \equiv 7 \bmod 12$, E is supersingular and $\tilde{E}$ is ordinary. This implies that E and $\tilde{E}$ are not isogenous, and $\mathrm{End}(A) = \mathrm{End}(E \times E) \times$

$\mathrm{End}(\tilde{E})$. Moreover, q is not a square, so both $\mathrm{End}(E)$ and $\mathrm{End}(\tilde{E})$ are imaginary quadratic rings, namely $\mathbb{Z}[\sqrt{-p}]$ and $\mathbb{Z}[\frac{-1+\sqrt{-3}}{2}]$, respectively (with again $p = \mathrm{char}(\mathbb{F}_q)$). Analogous to the previous case, one concludes that the part of $\mathrm{Jac}(C)$ corresponding to $E \times E$ contributes 0 to the trace of Frobenius on any twist of C. In particular, it follows that the number of points on such a twist equals the number of points on some twist of $\tilde{E}$. It is easily seen from the equations involved that in fact any of the (six) twists of $\tilde{E}$ over $\mathbb{F}_q$ occur.

For $q \equiv 5 \bmod 12$ we have that q is not a square and the elliptic curve $\tilde{E}$ is supersingular over $\mathbb{F}_q$. As before, this implies that $\tilde{E}$ contributes 0 to the trace of Frobenius on any twist of C over $\mathbb{F}_q$. In particular none of these twists is maximal. As an example, a Frobenius conjugacy class containing an automorphism $\alpha_{i,j}$ yields a twist given by an equation $\mu y^3 + 1 = \lambda x^4$. Since $y \mapsto \mu y^3$ defines a bijection on $\mathbb{F}_q$, both C and this twist have exactly $q+1$ rational points. The twists corresponding to a class which only contains automorphisms $\beta_{n,m,\ell}$ cannot be given by such a simple diagonal equation. One such twist, obtained by multiplying y by a fourth root of -3 in the equation for $C_{2\zeta^2-1}$, is given by

$$x^4 - 6x^2y^2 - 3y^4 + z^4 = 0.$$

In the remaining case $q \equiv 1 \bmod 12$, the field $\mathbb{F}_q$ contains a primitive 12th root of unity ζ. Put $\lambda := 16(2\zeta^3 - 4\zeta - 3)$ and $E_\lambda : \lambda y^2 = x^3 + 4x$. Combining the isomorphism $C \cong C_{2\zeta^2-1}$ presented in the first paragraphs of this section, with the map from $C_{2\zeta^2-1}$ to E given in Section 5, one obtains in fact over $\mathbb{F}_q$ a morphism $C \longrightarrow E_\lambda$ given as $(x:y:1) \mapsto (\xi, \eta)$, with

$$\xi := -\frac{((1-\zeta^3)x + (\zeta^3+\zeta^2-\zeta-1)y)^2}{(y-(\zeta^3-2\zeta-1)x)^2}$$

and

$$\eta := \frac{(1-\zeta^3)x + (\zeta^3+\zeta^2-\zeta-1)y}{(y-(\zeta^3-2\zeta-1)x)^3}.$$

This allows one to describe the number of points on each of the 14 twists of C over $\mathbb{F}_q$ in terms of (twists of) the elliptic curves $\tilde{E}$ and E_λ. As an example, for $q \equiv 1 \bmod 12$, we have

$$|C(\mathbb{F}_q)| = 2\,|E_\lambda(\mathbb{F}_q)| + \left|\tilde{E}(\mathbb{F}_q)\right| - 2q - 2.$$

Details of such a description are presented for the Dyck-Fermat curve in Section 7 and for the Klein curve in Section 8 below.

Remark 17. The discussion presented here shows that for $q \not\equiv 1 \bmod 12$, a twist of C over $\mathbb{F}_q$ attaining the Hasse-Weil bound does not exist. Moreover, a necessary condition is that $\tilde{E}$ and E_λ are (over some extension) isogenous, which happens precisely when the characteristic $p \equiv 11 \bmod 12$.

Vice versa, assume p is a prime number $\equiv 11 \bmod 12$ and $q = p^n \equiv 1 \bmod 12$, so $n = 2m$ is even. Note that under these conditions, $\zeta^p = \zeta - \zeta^3$ and hence $\lambda^p = 16(2\zeta^{3p} - 4\zeta^p - 3) = \lambda$, so $\lambda \in \mathbb{F}_p$. Both E_λ and $\tilde{E}$ are therefore supersingular elliptic curves over $\mathbb{F}_p$. It follows that

$$|C(\mathbb{F}_q)| = 2\,|E_\lambda(\mathbb{F}_q)| + \left|\tilde{E}(\mathbb{F}_q)\right| - 2q - 2 = q + 1 - 6(-p)^m.$$

In particular $C/\mathbb{F}_{p^n}$ attains the Hasse-Weil upper bound if and only if $p \equiv 11 \bmod 12$ and $n \equiv 2 \bmod 4$.

7. The Dyck-Fermat curve

In this section the twists of the Dyck-Fermat curve

$$C\ :\ x^4 + y^4 + z^4 = 0$$

over any finite field $\mathbb{F}_q$ of characteristic ≥ 5 will be described. This condition on the characteristic (see Section 4 above) ensures that $\mathrm{Aut}_{\bar{\mathbb{F}}_q}(C)$ has order 96. The automorphism group contains a normal subgroup $(\mu_4 \times \mu_4 \times \mu_4)/\Delta$ where Δ denotes the diagonal. This subgroup acts on the curve by multiplying the coordinates by 4th roots of unity. Another subgroup is S_3, acting by permuting the three coordinates. Together these two subgroups generate $\mathrm{Aut}_{\bar{\mathbb{F}}_q}(C)$, and in fact $\mathrm{Aut}_{\bar{\mathbb{F}}_q}(C) = (\mu_4 \times \mu_4 \times \mu_4)/\Delta \rtimes S_3$. In particular, elements of $\mathrm{Aut}_{\bar{\mathbb{F}}_q}(C)$ will be written as $((r_1, r_2, r_3), \alpha)$ with $r_j \in \mu_4$ and $\alpha \in S_3$.

This description makes it easy to calculate the Frobenius conjugacy classes. For $q \equiv 1 \bmod 4$, they are simply the 10 conjugacy classes in $\mathrm{Aut}_{\bar{\mathbb{F}}_q}(C)$. For $q \equiv 3 \bmod 4$ there are 6 Frobenius conjugacy classes. We summarize this discussion as part of Proposition 18 below.

Consider the elliptic curve E given by $2y^2 = x^3 - x$. Specializing the curves C_a in Section 4 to the case $a = -1$, we have

$$E \times E \times E \to \mathrm{Jac}(C),$$

with an explicit isogeny. Let $i \in \bar{\mathbb{F}}_q$ satisfy $i^2 = -1$ and let ι be the automorphism of $E \otimes \bar{\mathbb{F}}_q$ given by $\iota(x, y) = (-x, iy)$. Observe that the automorphism $\tau :\ (x : y : z) \mapsto (ix : y : z)$ of $C \otimes \bar{\mathbb{F}}_q$ yields the automorphism $\begin{pmatrix} \iota & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & \iota \end{pmatrix}$ of $E \times E \times E$. The action of S_3 on $E \times E \times E$ is already described in Section 4. In fact, in the notation of Section 4, the group S_3 is generated by the 3-cycle φ and the 2-cycle $\sigma := \psi^2\varphi\psi^{-1}$. This suffices to describe the trace of Frobenius for all twists of C in terms of the trace of the Frobenius $\pi \in \mathrm{End}(E)$.

Note that for $q \equiv 3 \bmod 4$ the elliptic curve E is supersingular. Since here q is not a square and we assume $q \geq 5$, this implies that the trace of Frobenius on all twists of $\mathrm{Jac}(C)$ over $\mathbb{F}_q$ is 0.

Proposition 18. *For $\mathbb{F}_q$ of characteristic ≥ 5, the twists of the Dyck-Fermat curve C given by $x^4 + y^4 + z^4 = 0$ over $\mathbb{F}_q$ are described in the following two tables. Here the first row presents the image $f(Fr) \in \mathrm{Aut}_{\bar{\mathbb{F}}_q}(C)$ for nonequivalent cocycles. For $q \equiv 1 \bmod 4$, a second row presents the trace of Frobenius on the Jacobian of the corresponding twist, in terms of the Frobenius endomorphism π of the elliptic curve given by $2y^2 = x^3 - x$. In case $q \equiv 3 \bmod 4$, all of the six twists C' of C over $\mathbb{F}_q$ have $|C'(\mathbb{F}_q)| = q + 1$.*

Case $q \equiv 3 \bmod 4$:

id	ψ	τ	σ	$\sigma\tau$	φ

Case $q \equiv 1 \bmod 4$:

id	τ^2	ψ	φ	τ	τ^3	$\tau\varphi^{-1}\tau^2\varphi$	$\sigma\tau$	$\sigma\tau^3$	$\psi\varphi^{-1}\tau^3\varphi$
$3\mathrm{tr}(\pi)$	$-\mathrm{tr}(\pi)$	$\mathrm{tr}(\pi)$	0	$-\mathrm{tr}(\pi) + 2\mathrm{tr}(\iota\pi)$	$-\mathrm{tr}(\pi) - 2\mathrm{tr}(\iota\pi)$	$\mathrm{tr}(\pi)$	$-\mathrm{tr}(\pi)$	$\mathrm{tr}(\iota\pi)$	$-\mathrm{tr}(\iota\pi)$

Remark 19. Proposition 18 implies that for a twist of C over $\mathbb{F}_q$ to attain the Hasse-Weil bound, one needs $q \equiv 1 \bmod 4$. Moreover, if this were to happen for a nontrivial twist of C, then E must be isogenous to a bi-quadratic twist of E. The latter condition is impossible when E is ordinary (since for ordinary E, Frobenius takes the form $a + b\iota$ and the bi-quadratic twists then have Frobenius of the form $\pm\iota(a+b\iota)$, which prevents the curves having the same number of points).

If E is supersingular and isogenous to its bi-quadratic twists and $q \equiv 1 \bmod 4$, then Frobenius on E is multiplication by an integer, and hence Frobenius on the bi-quadratic twists have trace 0. So also in this case, a nontrivial twist of C does not attain the Hasse-Weil bound.

We conclude that only C itself may attain the Hasse-Weil upper bound over $\mathbb{F}_q$. This happens if and only if $E/\mathbb{F}_q$ has the same property. This is the case whenever $q = p^n$ for a prime number $p \equiv 3 \bmod 4$ and an exponent $n \equiv 2 \bmod 4$.

8. The Klein curve

The final example to be discussed here, is the Klein curve

$$K \ : \ x^3y + y^3z + z^3x = 0.$$

Apart from texts already mentioned in Section 4, an excellent reference concerning this curve is [Elk99]. We recall the following properties of K. Throughout, we work over a field k of characteristic $\neq 7$ and $\neq 2$, $\neq 3$. Under these conditions, the equation given here defines a nonsingular curve of genus 3, with automorphism group over k^s the unique simple group of order 168.

Let ζ be a primitive 7th root of unity in some extension of k. Then $\zeta+\zeta^2-\zeta^3+\zeta^4-\zeta^5-\zeta^6$ is a square root of -7 which we write as $\sqrt{-7}$. The group $\mathrm{Aut}_{k^s}(K)$ is generated by three elements:

$$g\ :\ (x:y:z)\mapsto(\zeta^4x:\zeta^2y:\zeta z)$$

of order 7,

$$h\ :\ (x:y:z)\mapsto(y:z:x)$$

of order 3, and s of order 2 given by the matrix

$$\frac{-1}{\sqrt{-7}}\begin{pmatrix}\zeta-\zeta^6 & \zeta^2-\zeta^5 & \zeta^4-\zeta^3\\ \zeta^2-\zeta^5 & \zeta^4-\zeta^3 & \zeta-\zeta^6\\ \zeta^4-\zeta^3 & \zeta-\zeta^6 & \zeta^2-\zeta^5\end{pmatrix}.$$

Let E/k be the elliptic curve with equation $y^2+xy=x^3+5x^2+7x$. The endomorphism ring of this curve over k^s contains the ring of integers in $\mathbb{Q}(\sqrt{-7})$, and over k, the Jacobian $\mathrm{Jac}(K)$ is isogenous to a twist of $E\times E\times E$. More precisely, denoting (for k a finite field $\mathbb{F}_q$) the Frobenius endomorphism on E by π, one finds that the Frobenius in $\mathrm{End}(\mathrm{Jac}(K))$ corresponds to

$$\begin{pmatrix}0&1&0\\0&0&1\\1&0&0\end{pmatrix}^{o(q)}\begin{pmatrix}\pi&0&0\\0&\pi&0\\0&0&\pi\end{pmatrix}$$

in $\mathrm{End}(E\times E\times E)$, with $o(q):=\begin{cases}0 & \text{if } q\equiv\pm1 \bmod 7;\\ 1 & \text{if } q\equiv\pm2 \bmod 7;\\ 2 & \text{if } q\equiv\pm3 \bmod 7.\end{cases}$

Next, we describe the Frobenius conjugacy classes in $\mathrm{Aut}_{\overline{\mathbb{F}}_q}(K)$. Since the action of the qth power map Fr on $\mathrm{Aut}_{\overline{\mathbb{F}}_q}(K)$ is determined by $\zeta\mapsto\zeta^q$, this is a straightforward calculation in the group generated by g,h and s.

(1) In case $q\equiv1 \bmod 7$, the Galois action is trivial, and we count conjugacy classes. It is a well known fact that there are precisely 6 such classes here. As a consequence, for $q\equiv1 \bmod 7$ the Klein curve K has precisely 6 twists over $\mathbb{F}_q$. Representatives of the conjugacy classes and the cardinality of each class are as follows.

class of:	id	h	s	g	g^6	ghs
cardinality:	1	56	21	24	24	42

(2) In case $q\equiv2 \bmod 7$ there are 6 Frobenius conjugacy classes. The table below lists for each of them a representing element and the number of elements in the class.

class of:	id	h	s	gh	g^3h	gs
cardinality:	56	1	21	24	24	42

Hence for $q\equiv2 \bmod 7$, the Klein curve K has precisely 6 twists over $\mathbb{F}_q$.

(3) In case $q \equiv 3 \bmod 7$ there are 4 Frobenius conjugacy classes. The table below lists for each of them a representing element and the number of elements in the class.

class of:	id	h^2	g^2s	g^3s
cardinality:	56	28	42	42

Hence for $q \equiv 3 \bmod 7$, the Klein curve K has precisely 4 twists over $\mathbb{F}_q$.

(4) In case $q \equiv 4 \bmod 7$ there are 6 Frobenius conjugacy classes. The table below lists for each of them a representing element and the number of elements in the class.

class of:	id	h^2	s	g^2s	gh^2	g^3h^2
cardinality:	56	1	21	42	24	24

Hence for $q \equiv 4 \bmod 7$, the Klein curve K has precisely 6 twists over $\mathbb{F}_q$.

(5) In case $q \equiv 5 \bmod 7$ there are 4 Frobenius conjugacy classes. The table below lists for each of them a representing element and the number of elements in the class.

class of:	id	h	gs	g^2s
cardinality:	56	28	42	42

So for $q \equiv 5 \bmod 7$, the Klein curve K has precisely 4 twists over $\mathbb{F}_q$.

(6) Finally, also in case $q \equiv 6 \bmod 7$ there are 4 Frobenius conjugacy classes. The table below lists for each of them a representing element and the number of elements in the class.

class of:	id	h	gs	g^3s
cardinality:	28	56	42	42

Hence also for $q \equiv 6 \bmod 7$, the Klein curve K has precisely 4 twists over $\mathbb{F}_q$.

It remains to describe the trace of the Frobenius endomorphism on the Jacobian of each possible twist of K over $\mathbb{F}_q$. If $q \equiv 3, 5$, or $6 \bmod 7$, then q is not a square and moreover the prime $p = \operatorname{char} \mathbb{F}_q$ is inert in $\mathbb{Q}(\sqrt{-7})$ hence the elliptic curve $E/\mathbb{F}_q$ is supersingular. In particular, for each of the four twists of K over $\mathbb{F}_q$ the corresponding trace of Frobenius is zero, so K and its nontrivial twists have exactly $q+1$ rational points over $\mathbb{F}_q$.

If $q \equiv 1, 2, 4 \bmod 7$ five nontrivial twists K' of K over $\mathbb{F}_q$ exist. The description of the corresponding cocycles together with the relation between $\operatorname{End}(\operatorname{Jac}(K))$ and $\operatorname{End}(E \times E \times E)$ now shows:

Theorem 20. *Suppose $q \equiv 1, 2, 4 \bmod 7$. The Klein curve has exactly 6 twists over $\mathbb{F}_q$. Write π_E for the Frobenius endomorphism of the elliptic curve $E/\mathbb{F}_q$ given by $y^2 + xy = x^3 + 5x^2 + 7x$, and let $\alpha_{1,2}$ be the two elements of* $\operatorname{End}(E)$ *satisfying $\alpha^2 + \alpha + 2 = 0$.*

Then the Klein curve has exactly 6 *twists over* $\mathbb{F}_q$. *The traces of Frobenius corresponding to these twists are*

$$3\mathrm{tr}(\pi),\ 0,\ -\mathrm{tr}(\pi),\ \mathrm{tr}(\alpha_1\pi),\ \mathrm{tr}(\alpha_2\pi),\ \mathrm{tr}(\pi),$$

respectively.

Proof. The endomorphism algebra $\mathrm{End}(\mathrm{Jac}(K))\otimes\mathbb{Q}$ is isomorphic with the algebra of 3×3 matrices over $\mathbb{Q}(\sqrt{-7})$, which we write as

$$\mathrm{Mat}_{3,3}(\mathbb{Q}(\sqrt{-7})).$$

Thus $\mathrm{End}(\mathrm{Jac}(K))\otimes\mathbb{Q}$ acts on the 6-dimensional $\mathbb{Q}$ vector space

$$\mathbb{Q}(\sqrt{-7})\oplus\mathbb{Q}(\sqrt{-7})\oplus\mathbb{Q}(\sqrt{-7}),$$

and we have an embedding

$$\mathrm{End}(\mathrm{Jac}(K))\otimes\mathbb{Q}\subset\mathrm{Mat}_{6,6}(\mathbb{Q}).$$

The relative q-power Frobenius endomorphism $\pi'\in\mathrm{End}(\mathrm{Jac}(K))\otimes\mathbb{Q}$ of a twist K' of K is a root of the characteristic polynomial of the corresponding 6×6 matrix. The trace of π' equals minus the coefficient of the degree 5 term of this polynomial. Write tr for the trace form

$$\mathrm{tr}:\mathrm{Mat}_{3,3}(\mathbb{Q}(\sqrt{-7}))\to\mathbb{Q}(\sqrt{-7}),$$

and $\mathrm{tr}_{\mathbb{Q}(\sqrt{-7})/\mathbb{Q}}(\alpha)$ for the trace of an algebraic number $\alpha\in\mathbb{Q}(\sqrt{-7})$. The trace of π' as a 6 by 6 matrix with entries in $\mathbb{Q}$ is then equal to

$$\mathrm{tr}_{\mathbb{Q}(\sqrt{-7})/\mathbb{Q}}(\mathrm{tr}(\pi')).$$

In cases (1), (2) and (4) of pages 22-23, there are 6 conjugacy classes of $\mathrm{Aut}_{\overline{\mathbb{F}}_q}(K)$ which are represented by Frobenius conjugacy classes as a direct count of representatives shows. If π_E is the trace of Frobenius of the elliptic curve E, and $g\in\mathrm{Aut}_{\overline{\mathbb{F}}_q}(K)$ is a representative of a Frobenius conjugacy class, then the associated twist K' has trace

$$\mathrm{tr}_{\mathbb{Q}(\sqrt{-7})/\mathbb{Q}}(\pi_E\mathrm{tr}(g)).$$

The possible values of $\mathrm{tr}(g)$ are

$$3,0,-1,\alpha_1,\alpha_2,1,$$

hence the result. □

Remark 21. The results of this section imply that the Klein curve $K/\mathbb{F}_q$ attains the Hasse-Weil upper bound precisely when $q\equiv 1 \bmod 7$ and the elliptic curve $E/\mathbb{F}_q$ also attains this bound.
Now assume $q=p^{2m}$ for a prime $p\geq 5$. For K or some twist over $\mathbb{F}_q$ to attain the Hasse-Weil upper bound, a necessary condition is that the same is true for $E/\mathbb{F}_q$, which in turn implies that $p\equiv 3,5$ or $6 \bmod 7$. In the first two cases, for every odd m the nontrivial twist described in Theorem 20 attains the Hasse-Weil upper bound over $\mathbb{F}_{p^{2m}}$. In the remaining case, the Klein curve itself attains this bound over $\mathbb{F}_{p^{2m}}$ whenever m is odd.

In particular, for the Klein curve itself we have that it attains the Hasse-Weil upper bound over $\mathbb{F}_{p^{2m}}$ if and only if $p \equiv 6 \bmod 7$ and m is odd.

References

[AT02] Auer, Roland; Top, Jaap, *Some genus 3 curves with many points*, Algorithmic number theory (Sydney, 2002), 163–171, Lecture Notes in Comput. Sci., 2369, Springer-Verlag, Berlin, 2002.

[BST97] Buhler, J., Schoen, C., and Top, J., *Cycles, L-functions and triple products of elliptic curves*, J. reine angew. Math. **492** (1997), p. 93–133.

[Ci99] Ciani, Edgardo, *I vari tipi possibili di quartiche piane più volte omologiche armoniche*, Rend. del Circolo Mat. di Palermo **13** (1899), 347–373.

[CW10] Ciani, E. and Wieleitner, H., *Projektive Spezialisierungen von Kurven vierter und dritter Ordnung*, Chapter XIX in E. Pascal, Repertorium der höheren Mathematik, II: Geometrie, erste Hälfte, Grundlagen und ebene Geometrie. Teubner Verlag, Leipzig & Berlin, 1910.

[Dy80] Dyck, Walther, *Notiz über eine reguläre Riemann'sche Fläche vom Geschlechte drei und die zugehörige "Normalcurve" vierter Ordnung*, Math. Ann. **17** (1880), 510–516.

[Ed45] Edge, W.L., *A plane quartic curve with twelve undulations*, Edinburgh Math. Notes **35** (1945), 10–13.

[Elk99] Elkies, Noam D., The Klein quartic in number theory. The eightfold way, 51–101, Math. Sci. Res. Inst. Publ., 35, Cambridge Univ. Press, Cambridge, 1999.

[Ka95] Kantor, S., Theorie der endlichen Gruppen von eindeutigen Transformationen in der Ebene. Mayer & Müller, Berlin, 1895.

[KS96] Klassen, Matthew J. and Schaefer, Edward F., *Arithmetic and geometry of the curve $y^3 + 1 = x^4$*, Acta Arithm. **74** (1996), 241–257.

[Kl79] Klein, Felix, *Ueber die Transformation siebenter Ordnung der elliptischen Functionen*, Math. Ann. **14** (1879), 428–471.

[Mil86a] Milne, J. S. *Abelian varieties*, Arithmetic geometry (Storrs, Conn., 1984), 103–150, Springer-Verlag, New York, 1986

[Mil86b] Milne, J. S. *Jacobian varieties*, Arithmetic geometry (Storrs, Conn., 1984), 167–212, Springer-Verlag, New York, 1986.

[GIT65] Mumford, David, Geometric invariant theory. Ergebnisse der Mathematik und ihrer Grenzgebiete, Neue Folge, Band 34, Springer-Verlag, Berlin-New York, 1965.

[Neu79] Neumann, Peter M., *A lemma that is not Burnside's*, Math. Sci. **4** (1979), 133–141.

[Rub95] Rubin, Karl, *Modularity of mod 5 representations*, Modular forms and Fermat's last theorem (Boston, MA, 1995), 463–474, Springer-Verlag, New York, 1997.

[Ser79] Serre, Jean-Pierre, Local fields. Graduate Texts in Mathematics vol. 67, Springer-Verlag, New York, 1979.

[Ser83b] Serre, Jean-Pierre, *Sur le nombre des points rationnels d'une courbe algébrique sur un corps fini*, C. R. Acad. Sci. Paris Sér. I Math. **296** (1983), 397–402.

[Ser85] Serre, Jean-Pierre, Lectures on curves over finite fields. Notes taken by Fernando Gouvêa, Harvard university, 1985.

[Ser94] Serre, Jean-Pierre, Cohomologie Galoisienne. Cinquième édition, Lecture Notes in Mathematics, 5, Springer-Verlag, Berlin, 1997.

[Top89] Top, Jaap, Hecke L-series related with algebraic cycles or with Siegel modular forms. Ph.D. thesis, University of Utrecht, 1989.

[Ver83] Vermeulen, A.M., Weierstrass points of weight two on curves of genus three. Ph.D Thesis, University of Amsterdam, 1983.

[Wi97] Wiman, A., *Zur Theorie der endlichen Gruppen von birationalen Transformationen in der Ebene*, Math. Ann. **48** (1897), 195–240.

[Wr81] Wright, E.M., *Burnside's lemma: a historical note*, J. Combin. Theory Ser. B **30** (1981), 89–90.

Albert-Ludwigs-Universität Freiburg, Mathematisches Institut, Eckerstrasse 1, D-79104 Freiburg, Germany.

Johann Bernoulli Institute, Rijksuniversiteit Groningen, Nijenborgh 9, 9747 AG Groningen, the Netherlands.
E-mail address: stephen.meagher@math.uni-freiburg.de
E-mail address: j.top@rug.nl