COUNTING POINTS ON THE FRICKE-MACBEATH CURVE
OVER FINITE FIELDS

JAAP TOP AND CARLO VERSCHOOR

Abstract. The Fricke-Macbeath curve is a smooth projective algebraic curve
of genus 7 with automorphism group $\text{PSL}_2(\mathbb{F}_8)$. We recall two models of it
(introduced, respectively, by Maxim Hendriks and by Bradley Brock) defined
over $\mathbb{Q}$, and we establish an explicit isomorphism defined over $\mathbb{Q}(\sqrt{-7})$ between
these models. Moreover, we decompose up to isogeny over $\mathbb{Q}$ the Jacobian of
one of these models. As a consequence we obtain a simple formula for the
number of points over $\mathbb{F}_q$ on (the reduction of) this model, in terms of the
elliptic curve with equation $y^2 = x^3 + x^2 - 114x - 127$. Moreover, twists by
elements of $\text{PSL}_2(\mathbb{F}_8)$ of the curve over finite fields are described. The curve
leads to a number of new records as maintained on manypoints.org of curves
of genus 7 with many rational points over finite fields.

1. Introduction

It is well-known that an algebraic curve of genus $g > 1$ over $\mathbb{C}$ has at most
$84(g - 1)$ automorphisms. A curve attaining this bound is called a Hurwitz curve.
The corresponding Riemann surface can in this case be described as $\Gamma \backslash \mathcal{H}$ in which
$\Gamma$ is a normal subgroup of finite index in the triangle group $G_{2,3,7}$, acting in the
classical way on the complex upper half plane $\mathcal{H}$. See, e.g., §3.19 of Shimura’s paper
[Sh67] and §5.3 of the exposition by Elkies [El98] for details The plane curve with
equation $x^3y + y^3z + z^3 = 0$, named after Felix Klein who studied it in 1879 in his
paper [K79], is the unique example up to isomorphisms for genus $g = 3$. The next
example occurs for $g = 7$ and was introduced as a Riemann surface by Robert Fricke
in 1899 [F99]. Explicit equations realizing Fricke’s example as an algebraic curve,
were presented in 1965 by A.M. Macbeath [M65], see also W.L. Edge’s paper [Ed67]
which appeared two years later. Again, up to isomorphisms over $\mathbb{C}$ there is a unique
curve of genus 7 admitting 504 automorphisms; here and elsewhere it is called
the Fricke-Macbeath curve. Whereas Edge derives the equations first presented by
Macbeath by starting from the property that they need to define a curve in $\mathbb{P}^6$
having a given subgroup of order 504 in $\text{PGL}_7(\mathbb{C})$ as automorphism group, there is
an alternative, very natural way to find the curve, as is explained in a letter dated
24-vii-1990 of J-P. Serre to S.S. Abhyankar [Se90]. Namely, Serre observes that
$G = \text{PSL}_2(\mathbb{F}_8)$ is a transitive subgroup of the alternating group $A_9$ (which in fact
follows from the action of $G$ on the 9 points in $\mathbb{F}_8^1$). The stabilizer $S \subset G$ of
any of these 9 points then makes $X \to X/G$ the normal closure of $X/S \to X/G$,
where we denote the desired curve as $X$. Both $X/S$ and $X/G$ are rational curves,
and the ramification of the resulting degree 9 map $\mathbb{P}^1 \to \mathbb{P}^1$ is known and occurs
only over three points. This information suffices to determine the degree 9 map
explicitly, and hence to find the curve $X$.

The equations described by Macbeath (and explained in detail by Edge) define
a curve $M \subset \mathbb{P}^9$, given (with $\zeta_7$ a primitive 7th root of unity) by the ideal with
exactly this. He presented in his thesis [He13, p. 192–194] a curve [GTW14] is that it is possible to define the Fricke-Macbeath curve as an algebraic
A consequence of a very general criterion of Girondo, Torres-Teigell, and Wolfart generators
One readily calculates that this curve in $\mathbb{P}^2$ has no singular points at infinity. So indeed the equation defines a
As part of his PhD research, Maxim Hendriks in Eindhoven did
of the
Moreover Hendriks presents an explicit isomorphism between $M$ and $H$ (see also Theorem 1 below).
In §2.3 of a recent paper by Rubén Hidalgo [H15], another model over $\mathbb{Q}$ of the Fricke-Macbeath curve is mentioned. It is attributed to Bradley Brock, and given by the affine equation in two variables
One readily calculates that this curve in $\mathbb{A}^2$ has as singularities 14 nodes, and its closure in $\mathbb{P}^2$ has no singular points at infinity. So indeed the equation defines a curve of genus 7. Using a basis of the regular 1-forms on the normalization, one obtains an embedding of the curve in $\mathbb{P}^6$. The resulting curve $B \subset \mathbb{P}^6$ can be given as follows (here and in other calculations Magma [BCP97] was used).

$$B :$$

$$x_0x_2 + 12x_4^2 - x_4x_6,$$
$$-x_1^2 + x_0x_3 - 2x_5x_6,$$
$$x_0x_4 + 16x_3x_5 + 8x_2^2,$$
$$-x_1x_3 + x_0x_5 + \frac{1}{2}x_2x_6,$$
$$-x_2x_3 + 2x_2^2 + x_0x_6,$$
$$x_1x_2 + 12x_3x_5 + 4x_2^2,$$
$$-2x_3x_1 + x_1x_4 - 8x_5^2,$$
$$-x_3^2 + x_1x_5 + \frac{1}{2}x_4x_6,$$
$$-\frac{1}{2}x_3x_4 + \frac{1}{2}x_2x_5 + x_1x_6,$$
$$x_3^2 + 2x_4x_5 + 8x_6.$$
2. Results

First, we present explicit isomorphisms between the curves $M, H,$ and $B.$

**Theorem 1.** (Hendriks, [He13]) With notations as in the previous section and $\alpha := \zeta_7 + \zeta_7^{-1},$ an isomorphism $M \to H$ is given by $m \mapsto Am,$ with $7A =$

$$
\begin{pmatrix}
0 & 0 & \alpha^2 - \alpha - 2 & -\alpha^2 - \alpha - 1 & 0 & 2\alpha^2 - 1 & 0 \\
\alpha^2 - 2\alpha & 0 & 0 & 0 & 3\alpha + 1 & 0 & -\alpha^2 - 2\alpha + 1 \\
0 & 0 & -\alpha^2 - \alpha - 1 & -2\alpha^2 + 1 & 0 & \alpha^2 - \alpha - 2 & 0 \\
0 & 7\alpha & 0 & 0 & 0 & 0 & 0 \\
-\alpha^2 - 2\alpha + 1 & 0 & 0 & 0 & -\alpha^2 + 2\alpha & 0 & -3\alpha - 1 \\
0 & 0 & -3\alpha - 1 & -\alpha^2 + 2\alpha & 0 & \alpha^2 + 2\alpha - 1 & 0 \\
-3\alpha - 1 & 0 & 0 & 0 & \alpha^2 + 2\alpha - 1 & 0 & \alpha^2 - 2\alpha
\end{pmatrix}.
$$

**Theorem 2.** With notations as in the previous section, an isomorphism $B \to H$ is given by $b \mapsto A'b,$ with

$$A' = \frac{1}{2} \begin{pmatrix}
2 & -8 & 4 & -24 & 1 & 24 & 0 \\
2\sqrt{-7} & -4\sqrt{-7} & -2\sqrt{-7} & 0 & -\sqrt{-7} & 0 & -8\sqrt{-7} \\
6 & 4 & -2 & -16 & 3 & 16 & 0 \\
2\sqrt{-7} & -4\sqrt{-7} & -2\sqrt{-7} & -8\sqrt{-7} & -\sqrt{-7} & -8\sqrt{-7} & 16\sqrt{-7} \\
0 & -4\sqrt{-7} & -2\sqrt{-7} & -8\sqrt{-7} & 0 & -8\sqrt{-7} & -8\sqrt{-7} \\
-2 & 8 & -4 & -32 & -1 & 32 & 0 \\
2\sqrt{-7} & 0 & 0 & -8\sqrt{-7} & -\sqrt{-7} & -8\sqrt{-7} & -8\sqrt{-7}
\end{pmatrix}.
$$

Note that Theorems 1 and 2 imply that the three curves $M, H,$ and $B$ are isomorphic over $\mathbb{Q}(\zeta_7).$ Although both $H$ and $B$ are defined over $\mathbb{Q},$ they are not isomorphic over $\mathbb{Q}.$ This follows, e.g., from the fact that both have good reduction modulo 3, and $\#H(\mathbb{F}_3) = 3 \neq 5 = \#B(\mathbb{F}_3).$

From now on we focus on the model $H$ presented by Hendriks. Our aim is to describe the jacobian $Jac(H)$ up to isogenies defined over $\mathbb{Q},$ in terms of jacobians of certain quotients of $H.$ To this end, let $X \subset \mathbb{P}^2$ be the plane quartic of genus 3 defined by

$$X : \quad 5x^4 + 12x^3y + 6x^2y^2 - 4xy^3 + 4y^4 - 28x^3z + 16x^2yz - 24xy^2z + 16y^3z + 24x^2z^2 - 10y^2z^2 - 12xz^3 + 8y^3 + 3z^4.
$$

Furthermore let $E$ be the elliptic curve with equation

$$y^2 = x^3 + x^2 - 114x - 127.
$$

The curve $X$ defines the quotient of $H$ by the involution $\text{Diag}(-1, 1, -1, 1, -1, 1).$ It is the image of $H$ under $(x_0 : x_1 : x_2 : x_3 : x_4 : x_5 : x_6) \mapsto (x_0 : x_2 : x_5).$ The elliptic curve $E$ is obtained as a quotient of $H$ by a group of order 7. Such a quotient was also described by Klaus Wohlfahrt in the corrigendum to his paper [Wo86]. His elliptic curve is in fact the quadratic twist by $\sqrt{-7}$ of $E.$ The reader may verify that a very simple way to find the same elliptic curve as Wohlfahrt did, is by starting from the affine plane model of the Fricke-Macbeath curve given by Brock. Taking the quotient by $(x, y) \mapsto (\zeta_7 x, \zeta_7^{-1} y)$ yields Wohlfahrt’s elliptic curve.

**Theorem 3.** $Jac(H)$ is isogenous over $\mathbb{Q}$ to $Jac(X) \times Jac(X) \times E.$

The next goal will be to analyse $Jac(X).$ It turns out that $\text{Aut}(X)$ contains a group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z},$ with involutions defined over $\mathbb{Q}(\alpha).$ Moreover, these involutions are permuted by $\text{Gal}(\mathbb{Q}(\alpha)/\mathbb{Q}).$ Let $\sigma$ be a generator of this (cyclic) Galois group of order 3. The quotient of $X$ by one of the involutions turns out to be a genus one curve $C$ over $\mathbb{Q}(\alpha),$ with jacobian $E'$ isogenous, again over $\mathbb{Q}(\alpha),$ to $E.$ The action of $\sigma$ yields the jacobians of the three quotients of $X$ by the involutions. The restriction
of scalars $\text{Res}_{\mathbb{Q}(\alpha)/\mathbb{Q}}(E')$, which is over $\mathbb{Q}(\alpha)$ isomorphic to $E' \times \sigma(E') \times \sigma^2(E')$, is the abelian threefold over $\mathbb{Q}$ we look for.

**Theorem 4.** $\text{Jac}(X)$ is over $\mathbb{Q}$ isogenous to $\text{Res}_{\mathbb{Q}(\alpha)/\mathbb{Q}}(E')$, and the elliptic curves $E$ and $E'$ are isogenous over $\mathbb{Q}(\alpha)$.

A straightforward consequence of Theorem 4 is a formula for $\# X(\mathbb{F}_p)$, for $q = p^n$ and $p$ a prime $\neq 2, 7$:

**Corollary 5.** The curve $X$ has good reduction modulo every prime number $p \neq 2, 7$. If $q = p^n$ is a positive power of such a prime $p$, then

$$\# X(\mathbb{F}_q) = \begin{cases} q + 1 & \text{if } q \not\equiv \pm 1 \mod 7; \\ 3\# E(\mathbb{F}_q) - 2q - 2 & \text{if } q \equiv \pm 1 \mod 7. \end{cases}$$

Combining Theorem 3 and Corollary 5 leads to the main result of this paper:

**Theorem 6.** The curve $H$ has good reduction modulo every prime number $p \neq 2, 7$. If $q = p^n$ is a positive power of such a prime $p$, then

$$\# H(\mathbb{F}_q) = \begin{cases} \# E(\mathbb{F}_q) & \text{if } q \not\equiv \pm 1 \mod 7; \\ 7\# E(\mathbb{F}_q) - 6q - 6 & \text{if } q \equiv \pm 1 \mod 7. \end{cases}$$

The results described above are proven in the next section. In Section 4 we apply Theorem 6 to some particular prime powers $q$, resulting in various new records in the tables of curves with many points over finite fields. In the same section we describe twists of $H/\mathbb{F}_q$ and we show examples where these lead to new records as well.

Most results of this paper were obtained during the master’s project of the second author [V15], supervised by the first author.

3. Proofs

The statements in Theorem 1 and in Theorem 2 can be easily verified, so we omit this here. Instead, some comments are presented explaining how the isomorphisms were found. By construction, the curves $M, H,$ and $B$ are canonically embedded curves in $\mathbb{P}^6$. Hence an isomorphism between two of these curves is necessarily given by an element of $\text{PGL}_7(\mathbb{Q})$. Conjugation by this element then yields an isomorphism from the automorphism group of one curve to that of the other. By first determining such a conjugation, i.e., an $A \in \text{PGL}_7(\mathbb{Q})$ satisfying $A\alpha_1 = \alpha_2 A$ with $\alpha_1$ running over the generators of some subgroup of the automorphisms of one curve, and the $\alpha_2$ analogous generators of an isomorphic subgroup coming from the other curve, the isomorphisms were determined.

To make this explicit, consider the generators $T, W$ of $\text{Aut}(M) \subset \text{PGL}_7(\mathbb{Q})$, defined as

$$T = \begin{pmatrix} -1 & 0 & 0 & 1 & 1 & -1 & 0 \\ 0 & 0 & -1 & -1 & 1 & 0 & -1 \\ 0 & 1 & -1 & 1 & 0 & 1 & 0 \\ -1 & -1 & -1 & 0 & -1 & 0 & 0 \\ -1 & 1 & 0 & -1 & 0 & 0 & 1 \\ 1 & 0 & -1 & 0 & 0 & -1 & 1 \\ 0 & 1 & 0 & 0 & -1 & -1 & -1 \end{pmatrix}, \quad W = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$  

Then $T^3 = W^7 = (TW)^2 = \text{id}$. Corresponding generators $R, S$ of $\text{Aut}(H)$ satisfying $R^3 = S^7 = (SR)^2 = \text{id}$ one finds in the thesis of Hendriks [He13]. With $\alpha = \zeta_7 + \zeta_7^{-1}$
as before, they are
\[ \begin{pmatrix} 2\alpha^2 + 3\alpha - 7 & 3\alpha^2 + 4\alpha + 1 & 4\alpha^2 + 2\alpha - 6 & -\alpha^2 + \alpha + 2 & -4\alpha^2 - 3\alpha + 1 & -7\alpha^2 - 5\alpha + 10 & 3\alpha^2 - 3\alpha - 6 \\ 4\alpha^2 + 8\alpha - 4 & 4\alpha^2 + \alpha - 11 & -9\alpha^2 - 3\alpha + 14 & 2\alpha^2 + \alpha + 3 & -5\alpha^2 - 5\alpha + 2 & -2\alpha^2 + \alpha + 3 & 3\alpha^2 + 6\alpha + 5 \\ 2\alpha^2 - 4\alpha - 2 & 6\alpha^2 + 3\alpha - 9 & \alpha^2 + \alpha - 6 & -2\alpha^2 - \alpha + 3 & -\alpha^2 + \alpha + 2 & -2\alpha^2 + \alpha + 7 & 3\alpha^2 - \alpha + 4 \\ 14\alpha^2 + 7\alpha - 21 & 7\alpha + 7 & -7\alpha^2 + 7\alpha + 14 & 0 & 7\alpha^2 - 7\alpha + 7 & 0 & -7\alpha^2 - 7\alpha + 14 \\ 6\alpha^2 + 9\alpha - 7 & 5\alpha^2 + \alpha - 4 & -11\alpha^2 - 7\alpha + 16 & 2\alpha^2 - \alpha + 1 & -3\alpha^2 - 4\alpha - 1 & 1\alpha^2 + 2\alpha - 1 & 5\alpha - 3 \\ 6\alpha^2 - 10 & 3\alpha^2 - 5 & 4\alpha^2 + 8\alpha - 4 & -\alpha^2 - 3 & -4\alpha^2 + 2 & -3\alpha^2 + 4 & 3\alpha^2 + 5 \\ 4\alpha^2 + 11\alpha - 3 & 5\alpha^2 + 13 & -8\alpha^2 - 4\alpha + 12 & -\alpha^2 + \alpha - 2 & -6\alpha^2 - 5\alpha + 13 & \alpha^2 - 2\alpha - 2 & -\alpha^2 + 3\alpha - 2 \end{pmatrix} \]

and
\[ S := \begin{pmatrix} -\alpha^2 - 4 & 2\alpha^2 + \alpha - 3 & 0 & \alpha^2 + 3 & -\alpha^2 - 2\alpha + 1 & \alpha^2 - 4 \\ 3\alpha^2 + 1 & -\alpha^2 - 5 & 2\alpha^2 + 2\alpha - 5 & 0 & -\alpha + 2 & -2\alpha^2 - \alpha + 3 & -\alpha + 2 \\ 2\alpha^2 + 3 & -\alpha^2 - 4 & 2\alpha^2 + \alpha - 3 & 0 & \alpha^2 + 3 & -\alpha^2 - 2\alpha + 1 & \alpha^2 - 4 \\ -7\alpha^2 + 14 & 0 & 0 & 0 & -7 & 0 & 0 \\ -\alpha^2 + 2\alpha - 3\alpha - 1 & -2\alpha^2 - \alpha + 3 & \alpha^2 - 4 & -\alpha^2 + \alpha + 2 & -\alpha + 2 & 2\alpha^2 + 3\alpha + 3 \\ 2\alpha^2 + 3\alpha + 5\alpha^2 + 3\alpha - 10 & -\alpha^2 + \alpha + 2 & 0 & -2\alpha^2 - 5\alpha + 4 & -\alpha^2 - \alpha - 1 & -2\alpha^2 + 2\alpha + 4 \\ \alpha^2 + 2\alpha - 1 & -2\alpha^2 - 2\alpha - 3\alpha^2 - 4\alpha - 4 & -\alpha^2 - \alpha - 1 & -3\alpha^2 + 5 & -\alpha^2 - 10 & 2\alpha^2 - 3\alpha - 3 \end{pmatrix} \]

Solving for the matrix \( A \) in the linear equations \( RA = AT, SA = AW \) then results in the desired isomorphism.

In the case of the curves \( B \) and \( H \), the only obvious automorphisms of \( B \) form a dihedral group of order 14. On the plane model, this group is generated by \( (x, y) \mapsto (y, x) \) and \( (x, y) \mapsto (\zeta x, \zeta^4 y) \). On \( B \) this yields the matrices
\[ D := \text{Diag}(\zeta_7^3, \zeta_7^2, \zeta_7, \zeta_7^2, \zeta_7^4, 1) \]

and
\[ F := \begin{pmatrix} 0 & 0 & 0 & -2 & 0 & 0 \\ 0 & 0 & 2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ -\frac{7}{2} & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix} \]

A corresponding dihedral group in \( \text{Aut}(H) \) is the one with generators
\[ \tau := (S^{-1}RS^{-1})^2RS = \text{Diag}(-1, 1, 1, 1, 1, -1, 1) \]

and \( L := (S^{-2}R)^2S^{-1} \), given by
\[ \begin{pmatrix} -4\alpha^2 - \alpha + 4 & 3\alpha^2 - 12 & 4\alpha^2 + 2\alpha - 6 & -\alpha^2 + \alpha + 2 & 5\alpha + 4 & \alpha^2 + 5\alpha - 5\alpha^2 - 3\alpha + 12 \\ -2\alpha^2 - 6\alpha + 6 & -3\alpha - 1 & 7\alpha^2 + 7\alpha - 7 & -\alpha - 5 & -7\alpha^2 - 3\alpha + 13 & -2\alpha^2 + \alpha + 1 & 7\alpha^2 + 4\alpha - 8 \\ 3\alpha^2 + 4\alpha - 2 & -2\alpha^2 - 5\alpha - 3 & 5\alpha^2 - \alpha - 11 & -2\alpha^2 + \alpha + 3 & 3\alpha^2 + 3\alpha - 3 & -4\alpha^2 - \alpha + 7 & -5\alpha^2 + 6 \\ -7\alpha & -7\alpha^2 + 7\alpha - 7 & 7 & -\alpha^2 + 7 & 7\alpha^2 + 7\alpha - 14 & \alpha^2 + 3\alpha - 3 \alpha^2 + 3\alpha + 2 \\ 4\alpha^2 + 8\alpha - 4 & 5\alpha^2 + 4\alpha - 12 & 2\alpha^2 + \alpha - 6 & -\alpha^2 + 4 & -6\alpha^2 - 2\alpha + 14 & -2\alpha^2 + 2\alpha - 1 & -\alpha^2 + 6\alpha + 6 \\ 2\alpha^2 - \alpha - 6 & 3\alpha^2 - 4\alpha - 4 & 6\alpha^2 + 4\alpha - 4 & \alpha^2 + 6 & -4\alpha^2 + 3\alpha + 10 & -\alpha^2 + 4\alpha - 3 & 3\alpha^2 + 3\alpha - 4 \end{pmatrix} \]

Solving the system \( \tau A' = A'F \), \( LA' = A'D \) for the matrix \( A' \) yields the map given in Theorem 2.

We will now prove Theorem 3. Denote \( \pi : (x_0 : \ldots : x_0) \mapsto (x_0 : x_2 : x_5) \), with \( \pi(H) = X \). Let \( \omega_1, \omega_2, \omega_3 \) be a basis for the space of regular differentials \( H^0(X, \Omega^1) \). A calculation shows that \( \pi \omega_1, \pi^* \omega_2, \pi^* \omega_3, \tau^* \pi^* \omega_1, \tau^* \pi^* \omega_2, \tau^* \pi^* \omega_3 \) are linearly independent in \( H^0(H, \Omega^1) \). Hence
\[ (\pi, \pi\tau) : H \to X \times X \]

induces a homomorphism \( \text{Jac}(X) \times \text{Jac}(X) \to \text{Jac}(H) \) with finite kernel. Then the cokernel is an abelian variety of dimension 1 defined over \( \mathbb{Q} \), i.e., it is an elliptic curve over \( \mathbb{Q} \). We briefly sketch two methods to find an equation for this elliptic curve (in the first case, up to isogeny over \( \mathbb{Q} \)).

For the first method, observe that the curve \( B \) (and hence also \( H \)) has good reduction except at the primes 2 and 7. A convenient way to verify this, is by using the plane model of \( B \). A consequence of this is, that the desired elliptic curve has good reduction away from 2 and 7. So its conductor divides \( 2^s \cdot 7^t \). Moreover, by
construction the number of rational points on this elliptic curve over \( \mathbb{F}_p \) for a prime \( p \neq 2, 7 \) equals

\[
\#H(\mathbb{F}_p) - 2\#X(\mathbb{F}_p) + 2p + 2.
\]

This information suffices to determine the correct isogeny class among the finitely many possible ones.

Alternatively, and more geometrically, take \( \rho := (SR^{-1}S)^3 \) which is an automorphism defined over the ground field, of order 3. A calculation (compare [V15, p. 13-15]) reveals that \( H/\langle \rho \rangle \) is a curve of genus 1, given by \( y^2 = -7t^4 - 28t^3 - 56t^2 - 28 \).

The Jacobian of this curve is our curve \( E \). Since \( \rho^* \) fixes no differentials in the subspace of \( H^0(X, \Omega^1) \) spanned by \( \pi^*\omega_1, \pi^*\omega_2, \pi^*\omega_3, \tau^*\pi^*\omega_1, \tau^*\pi^*\omega_2, \tau^*\pi^*\omega_3 \), it follows that \( \text{Jac}(H) \sim \text{Jac}(X) \times \text{Jac}(X) \times E \).

Next we prove Theorem 4. For this, one observes that \( X \) admits over \( \mathbb{Q}(\alpha) \) the involution given by

\[
A := \frac{1}{7} \begin{pmatrix}
-4\alpha^2 - 4\alpha + 3 & -2\alpha^2 + 2\alpha + 4 & 4\alpha^2 + 2\alpha - 6 \\
-4\alpha^2 - 2\alpha + 6 & 2\alpha^2 + 2\alpha - 5 & 2\alpha^2 + 4\alpha - 2 \\
2\alpha^2 - 2\alpha - 4 & 6\alpha + 2 & 2\alpha^2 + 2\alpha - 5
\end{pmatrix}.
\]

Moreover, \( A \) and its conjugates \( \sigma(A) \) and \( \sigma^2(A) \) generate a group of automorphisms of \( X \) isomorphic to \( \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \). The quotient of \( X \) by any nontrivial element of this group is an elliptic curve over \( \mathbb{Q}(\alpha) \), and the three elliptic curves obtained in this way are obviously conjugate. There are no nontrivial regular differentials on \( X \) fixed by all three involutions. This suffices to conclude that \( \text{Jac}(X) \) is isogenous over \( \mathbb{Q} \) to the restriction of scalars of any of the three elliptic curves. The elliptic curve \( E \) has its three points of order 2 defined over \( \mathbb{Q}(\alpha) \). The 2-isogenies resulting from this, turn out to have as image curves exactly the three elliptic curves we found as quotients of \( X \). This proves Theorem 4.

Corollary 5 is an immediate consequence of Theorem 4. The statement concerning good reduction is easily verified. In the case \( q \equiv \pm 1 \mod 7 \), all 7-th roots of unity exist in \( \mathbb{F}_q \) and hence \( \mathbb{F}_q \) contains the residue class field at the primes dividing \( q \) of \( \mathbb{Q}(\alpha) \). As a consequence, \( \text{Jac}(X) \) is isogenous over \( \mathbb{F}_q \) to \( E \times E \times E \), from which the formula for the number of points in this case is immediate. For \( q \neq \pm 1 \mod 7 \), the residue class field of \( \mathbb{Q}(\alpha) \) at primes dividing \( q \) is not contained in \( \mathbb{F}_q \) but in its cubic extension. Hence the \( q \)-th power Frobenius permutes the reductions of the three curves \( E', \sigma(E'), \) and \( \sigma^2(E') \). This implies that the trace of Frobenius on \( \text{Res}_{\mathbb{Q}(\alpha)/\mathbb{Q}}(E') \) is zero, implying the remaining formula.

This completes the proof of the results presented in Section 2.
4. Examples and twists

The website [http://manypoints.org/](http://manypoints.org/) lists, for small genera g and small cardinalities q of a finite field, an upper bound up for the cardinality #C(𝔽q) of any smooth, complete and absolutely irreducible curve C of genus g defined over 𝒋. In many instances this is the Hasse-Weil-Serre bound q + 1 + gm, in which m is the largest integer ≤ √q. In case a curve reaching this bound is known to exist, this means the number Nr(g), denoting the maximum over all such cardinalities #C(𝔽q) for fixed g, q is determined. If no curve reaching the upper bound is known then the tables aim to list an example with at least up/√q rational points. We now list the cases in which the curve H provides such an example. Instances where an example with at least as many points is known, will be ignored. Somewhat surprisingly, even with q ≠ ±1 mod 7, in which case Theorem 3 shows that H has (only) as many rational points as the elliptic curve E, some new entries were found.

| q   | 3³  | 5³  | 5⁵  | 11⁵ | 13²  | 13³  | 13⁴  | 13⁵  |
|-----|-----|-----|-----|-----|------|------|------|------|
| up  | 95  | 277 | 3903| 166666 | 352  | 2849 | 30928 | 379820 |
| [up/√q] | 68  | 196 | 2760 | 117851 | 249  | 2015 | 21870 | 268574 |
| #H(𝔽q) | 84  | 252 | 3183 | 161625 | 324  | 2688 | 27540(*) | 362880(*) |
| q   | 17³ | 17⁵ | 19⁴ | 19⁵ | 29   | 97   |
| up  | 5892 | 1436539 | 135376 | 2498129 | 100  | 231  |
| #H(𝔽q) | 4167 | 1015787 | 95726  | 1766444 | 71   | 164  |

In a sense the ‘smallest’ example here is #H(𝔽₂₇) = 84. The previous record for q = 27 and g = 7 was obtained by Sémirat [Sem00] in 2000, who found an example having 82 rational points. The three marked (*) entries show examples which we will improve now, as follows.

A natural attempt to obtain more examples with many points from the curve H, is to consider twists of it over ℚ, i.e., curves over the same field which are isomorphic to H over some extension field. We refer to [MT] for some general theory concerning twists. The twists over ℚ are in 1–1 correspondence with the set H¹(Ḡ(𝔽q/ℚ), Aut(H)), and the latter set allows a natural bijection to the set of ‘Frobenius conjugacy classes’ in Aut(H).

In our case, we consider H¹(Ḡ(𝔽q/ℚ), G), with G ⊂ PGL₇(𝔽q) the simple group of order 504 acting as automorphisms on H. These automorphisms are defined over 𝒋ζ + ζ⁻¹ with ζ a primitive 7th root of unity. Hence the Galois action on G is trivial precisely when q ≡ ±1 mod 7. In this case, Frobenius conjugacy classes coincide with ordinary conjugacy classes, and there are 9 of these. For q ≠ ±1 mod 7 a calculation with Magma shows that there exist only 3 Frobenius conjugacy classes.

If an automorphism β defines some Frobenius conjugacy class, then the corresponding cocycle class is represented by the cocycle defined by Frobq ↦ β. It defines a twist Htw, and by construction rational points on this twist correspond to points P ∈ H(𝔽q) such that β(Frobq(P)) = P. This allows one to calculate, for given q and β, the number of rational points #Htw(𝔽q).

Ignoring the trivial twist which results in the curve H itself, we can improve 3 of the records presented in the earlier table. They are given below.

1. \(q = 13^4 \equiv 1 \mod 7\). The (cubic) twist corresponding to Frobq ↦ R has 28854 rational points. This exceeds #H(𝔽₁₃⁴) = 27540.
2. \(q = 13^5 \equiv -1 \mod 7\). The quadratic twist corresponding to the cocycle Frobq ↦ τ = (S⁻¹RS⁻¹)²RS has 372496 rational points, while #H(𝔽₁₃⁵) = 362880.
(3) (Again) \( q = 13^5 \equiv -1 \mod 7 \). The cubic twist corresponding to the cocycle \( \text{Frob}_q \mapsto \tau = (S^{-1}RS^{-1})^2RS \) has 130969 rational points, whereas \( \#H(F_{13^5}) = 129675 \).

Using the Sage code from appendix A.2.3 of [V15] one can calculate explicit models for the desired twists. As an example, the quadratic twist using the automorphism \((x,y) \mapsto (y,x)\) of the affine curve
\[
1 + 7xy + 21x^2y^2 + 35x^3y^3 + 28x^4y^4 + 2x^7 + 2y^7 = 0
\]
the twist over \( F_q(\sqrt{d})/F_q \) is given by:
\[
7d^4x^8 + 2d^4x^7 - 28d^3x^6y^2 + 35d^3x^6 + 42d^3x^5y^2 + 42d^2x^4y^4 - 105d^3x^4y^2 \\
+ 70d^2x^3y^4 - 28dx^2y^6 + 84d^2x^4 + 105d^2x^2y^4 + 14dxy^6 + 7y^8 - 168d^2x^2y^2 - 35dy^6 \\
+ 112d^2x^2 + 84d^2y^4 - 112d^2y^2 + 64d^4 = 0.
\]

References

[BCP97] W. Bosma, J.J. Cannon, and C. Playoust, The Magma algebra system. I. The user language, J. Symbolic Comput., 24 (1997), 235–265.

[Ed67] W. L. Edge, A canonical curve of genus 7, Proc. LMS (3) 17 (1967), 207–225.

[Elk98] N. D. Elkies, Shimura curve computations, in: ‘Algorithmic number theory’ (Portland, OR, 1996, J.P. Buhler, ed.), 1—47, Lecture Notes in Comput. Sci. 1423, Springer-Verlag, Berlin, 1998.

[F99] R. Fricke, Ueber eine einfache Gruppe von 504 Operationen, Math. Ann. 52 (1899), 321–339.

[GTW14] E. Girondo, D. Torres-Teigell, and J. Wolfart, Fields of definition of uniform dessins on quasiplatonic surfaces, in: ‘Riemann and Klein surfaces, automorphisms, symmetries and moduli spaces’, 155–170, Contemp. Math. 629, AMS, Providence, 2014.

[H13] M. Hendriks, Platonic Maps of Low Genus. PhD thesis, Eindhoven University of Technology, 2013.

[He13] R. A. Hidalgo, Edmonds maps on the Fricke-Macbeath curve, Ars Math. Contemp. 8 (2015), 275–289.

[K79] F. Klein, Ueber die Transformation siebenter Ordnung der elliptischen Funktionen, Math. Ann. 14 (1879), 428–471.

[M65] A. M. Macbeath, On a curve of genus 7, Proc. LMS (3) 15 (1965), 527–542.

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

[Sém00] S. Sémirat, 2-Extensions with many points, preprint, 2000, [http://arxiv.org/abs/math/0011067v1](http://arxiv.org/abs/math/0011067v1).

[Se90] J-P. Serre, A letter as an Appendix to the Square-Root Parameterization Paper of Abhyankar, Chapter 3 (pages 85–88) in ‘Algebraic Geometry and its Applications’ (C.L. Bajaj, ed.), Springer-Verlag, New York, 1994.

[Sh67] G. Shimura, Construction of class fields and zeta functions of algebraic curves, Ann. of Math. 85 (1967), 58–159.

[V15] C. Verschoor, Twists of the Klein Curve and of the Fricke Macbeath Curve. Master’s thesis, University of Groningen, 2015. [http://irs.ub.rug.nl/dbi/55e5a09c6f723](http://irs.ub.rug.nl/dbi/55e5a09c6f723).

Wohlfahrt, Macbeath’s Curve and the Modular Group, Glasgow Math. J. 27 (1985), 239–247; Corrigendum Glasgow Math. J. 28 (1986), 241–241.

Johann Bernoulli Institute, University of Groningen, P.O.Box 407, 9700 AK Groningen, the Netherlands

E-mail address: j.top@rug.nl
E-mail address: carlovmm@gmail.com