Automorphisms of hyperelliptic modular curves $X_0(N)$ in positive characteristic

Aristides Kontogeorgis and Yifan Yang

Abstract

We study the automorphism groups of the reduction $X_0(N) \times \bar{\mathbb{F}}_p$ of a modular curve $X_0(N)$ over primes $p \nmid N$.

1. Introduction

Let $\mathcal{X} \to S$ be a family of curves of genus $g \geqslant 2$ over a base scheme S. For every point $P : \operatorname{Spec} k \to S$, we will consider the *absolute* automorphism group of the fibre P to be the automorphism group $\operatorname{Aut}_{\bar{k}}(\mathcal{X} \times_S \operatorname{Spec} \bar{k})$, where $\bar{k}$ is the algebraic closure of k. Any automorphism σ acts like the identity on $\bar{k}$, so in our setting there is no $\operatorname{Gal}(\bar{k}/k)$ contribution to the automorphism group of any special fibre. The following theorem due to Deligne and Mumford [7, Lemma I.12] compares the automorphism groups of the generic and special fibres.

PROPOSITION 1.1 [7]. *Consider a stable curve $\mathcal{X} \to S$ over a scheme S and let $\mathcal{X}_\eta$ denote its generic fibre. Every automorphism $\phi : \mathcal{X}_\eta \to \mathcal{X}_\eta$ can be extended to an automorphism $\phi : \mathcal{X} \to \mathcal{X}$.*

Of course, the special fibre of $\mathcal{X}$ might possess automorphisms that cannot be lifted to the generic fibre. For example, the Fermat curve

$$x^{p^s+1} + y^{p^s+1} + z^{p^s+1} = 0$$

can be considered as a stable curve over $\operatorname{Spec} \mathbb{Z}[1/(p^s+1)]$ and has automorphism group $(\mu_n \times \mu_n) \rtimes S_3$ for all geometric fibres above the primes $q \neq p$ but $\operatorname{PGU}(3, p^{2s})$ for the prime p [19, 32]. A special fibre $\mathcal{X}_p := \mathcal{X} \times_S S/p$ with $\operatorname{Aut}(\mathcal{X}_p) > \operatorname{Aut}(\mathcal{X}_\eta)$ will be called *exceptional*. In general, we know that there are finitely many exceptional fibres and it is an interesting problem to determine exactly the exceptional fibres.

There are some results towards this problem for some curves of arithmetic interest. Adler [1] and Rajan [24] proved for the modular curves $X(N)$ that $X(11)_3 := X(11) \times_{\operatorname{Spec} \mathbb{Z}} \operatorname{Spec} \mathbb{F}_3$ has the Mathieu group M_{11} as the full automorphism group. Ritzenthaler [25] and Bending et al. [3] studied the automorphism groups of the reductions $X(q)_p$ of modular curves $X(q)$ for various primes p. It turns out that the reduction $X(7)_3$ of $X(7)$ at the prime 3 has an automorphism group $\operatorname{PGU}(3, 3)$, and $X(7)_3$ and $X(11)_3$ are the only cases where $\operatorname{Aut} X(q)_p > \operatorname{Aut} X(q) \cong \operatorname{PSL}(2, p)$.

In this paper we will investigate some modular curves of the form $X_0(N)$. Igusa [15] proved that $X_0(N)$ has a non-singular projective model which is defined by equations over $\mathbb{Q}$ whose reduction modulo primes $p, p \nmid N$ is also non-singular, or in a more abstract language that there is a proper smooth curve $\mathcal{X}_0(N) \to \mathbb{Z}[1/N]$ so that for $p \in \operatorname{Spec} \mathbb{Z}[1/N]$ the reduction $\mathcal{X}_0(N) \times_{\operatorname{Spec} \mathbb{Z}} \mathbb{F}_p$ is the moduli space of elliptic curves with a fixed cyclic subgroup of order N.

The automorphism group of the curve $X_0(N)$ at the generic fibre is now well understood. Let us call an automorphism σ of $X_0(N)$ *modular* if σ arises from the normalizer of $\Gamma_0(N)$ in $\mathrm{SL}(2, \mathbb{R})$; then the results of [**8**, **16**, **22**] can be summarized as follows.

THEOREM 1.2 [**8**, **16**, **22**]. *Assume that $X_0(N)$ has genus $g \geqslant 2$. Then all the automorphisms of $X_0(N)$ are modular, with only two exceptions, namely the cases $N = 37, 63$, which have extra non-modular involutions.*

REMARK 1.3. Note that if $4 \nmid N$ and $9 \nmid N$, then all modular automorphisms are of the Atkin–Lehner type [**2**, Theorem 8]. In particular, if $4 \nmid N$ and $9 \nmid N$, then the automorphism group is an elementary abelian 2-group.

Denote by $A(N, 0)$ the absolute automorphism group of $\mathcal{X}_0(N)$ at the generic fibre and by $A(N, p)$ the absolute automorphism group at the reduction at the prime p. The problem of determining the exact primes for which $A(N, p) > A(N, 0)$ seems difficult in general. However, when $X_0(N)$ is hyperelliptic, the situation is relatively simple because the function field of a hyperelliptic curve has a unique genus zero subfield of degree 2, and the problem of determining the automorphism group of a hyperelliptic curve is essentially the same as that of determining the automorphisms of a projective line that permute a set of marked points. Therefore, as a starting point for our general problem of studying automorphisms of $X_0(N)$ in positive characteristics, in this note we will investigate the automorphism groups of hyperelliptic modular curves $X_0(N)$.

THEOREM 1.4. *Table 1 is the complete list of integers N and primes p such that the reduction of the hyperelliptic modular curve $X_0(N)$ modulo p has exceptional automorphisms.*

In the table, the notation D_n denotes the dihedral group of order $2n$,

$$A := \langle a, b, c \mid c^2, ba^{-2}b^{-1}a^{-1}, b^{-1}a^3ba^{-1}, ba^{-1}cb^{-1}a^{-1}ca^{-1}c, (a^{-1}b^{-1}cb^{-1})^2 \rangle$$

is a group of order 672,

$$B := \langle a, b, c \mid c^2, a^{-5}, b^{-1}a^{-2}ba, (cb^{-1})^3, a^{-1}bca^2cac \rangle$$

is a group of order 240 and

$$V_n = \langle x, y \mid x^4, y^n, (xy)^2, (x^{-1}y)^2 \rangle$$

is a group of order $4n$. Moreover, in the case of $X_0(37)$ in characteristic 2, the notation E_{32-} represents the extraspecial group $E_{32-} = (D_4 \times Q_8)/\langle(a, b)\rangle$, where a and b denote the non-trivial elements of the centers of D_4 and Q_8, respectively. (An *extraspecial group* H is a p-group such that the center Z is cyclic of order p and the quotient group H/Z is a non-trivial elementary abelian p-group.)

2. Automorphisms in characteristic $p \neq 2$

According to [**23**], there are exactly nineteen values of N such that $X_0(N)$ is hyperelliptic. The equations of the form $y^2 = f(x)$ for hyperelliptic $X_0(N)$ have been computed by several authors [**9**, **11**, **31**]. They are tabulated in Table 2, along with their modular automorphisms. Here, for a divisor e of N with $(e, N/e) = 1$, we let w_d be the Atkin–Lehner involution corresponding to the normalizer

$$\begin{pmatrix} ae & b \\ cN & de \end{pmatrix}, \quad ade - bcN/e = 1$$

of $\Gamma_0(N)$. For $X_0(28)$ and $X_0(40)$, the notation $w_{1/2}$ represents the automorphism coming from the normalizer

$$\begin{pmatrix} 1 & 1/2 \\ 0 & 1 \end{pmatrix}.$$

The notation $w_{1/4}$ in the case $X_0(48)$ carries a similar meaning.

These models are not the Igusa models. They have a singularity at infinity but are smooth otherwise. The automorphism group of a non-singular curve is a birational invariant and one can work with singular models of the corresponding function fields. But, one has to be careful if one wants to compute reductions out of the singular model.

TABLE 1. *Automorphism groups of $X_0(N)$ in positive characteristics.*

N	Genus	Generic Aut	Exceptional primes	Exceptional Aut
22	2	$(\mathbb{Z}/2\mathbb{Z})^2$	3, 29	D_6
			101	D_4
23	2	$\mathbb{Z}/2\mathbb{Z}$	3, 13, 29, 43, 101, 5623	$(\mathbb{Z}/2\mathbb{Z})^2$
26	2	$(\mathbb{Z}/2\mathbb{Z})^2$	7, 31	D_6
			41, 89	D_4
28	2	D_6	3	$GL(2,3)$
			5	B
			11	V_6
29	2	$\mathbb{Z}/2\mathbb{Z}$	19	D_4
			5, 67, 137, 51241	$(\mathbb{Z}/2\mathbb{Z})^2$
30	3	$(\mathbb{Z}/2\mathbb{Z})^3$	23	V_8
31	2	$\mathbb{Z}/2\mathbb{Z}$	3	D_4
			5, 11, 37, 67, 131, 149	$(\mathbb{Z}/2\mathbb{Z})^2$
33	3	$(\mathbb{Z}/2\mathbb{Z})^2$	2	$GL(2,2) \times (\mathbb{Z}/2\mathbb{Z})$
			19	$(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/4\mathbb{Z})$
			47	$(\mathbb{Z}/2\mathbb{Z})^3$
35	3	$(\mathbb{Z}/2\mathbb{Z})^2$	—	—
37	2	$(\mathbb{Z}/2\mathbb{Z})^2$	2	$E_{32-} \rtimes (\mathbb{Z}/5\mathbb{Z})$
			7, 31	D_6
			29, 61	D_4
39	3	$(\mathbb{Z}/2\mathbb{Z})^2$	5	$(\mathbb{Z}/2\mathbb{Z})^3$
			29	$(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/4\mathbb{Z})$
40	3	$(\mathbb{Z}/2\mathbb{Z}) \times D_4$	3	V_8
41	3	$\mathbb{Z}/2\mathbb{Z}$	17	$(\mathbb{Z}/2\mathbb{Z})^2$
46	5	$(\mathbb{Z}/2\mathbb{Z})^2$	3	$(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/4\mathbb{Z})$
47	4	$\mathbb{Z}/2\mathbb{Z}$	—	—
48	3	$(\mathbb{Z}/2\mathbb{Z}) \times S_4$	7	$A, |A| = 672$
50	2	$(\mathbb{Z}/2\mathbb{Z})^2$	3	D_6
			37	D_4
59	5	$\mathbb{Z}/2\mathbb{Z}$	—	—
71	6	$\mathbb{Z}/2\mathbb{Z}$	—	—

PROPOSITION 2.1. *Let $y^2 = f(x)$, where $f(x) \in \mathbb{Z}[x]$ is a polynomial with integer coefficient such that $\deg(f) \equiv 0 \bmod 2$.*

TABLE 2. *List of hyperelliptic curves $X_0(N)$.*

N	Equation/Automorphisms
22	$y^2 = (x^3 + 4x^2 + 8x + 4)(x^3 + 8x^2 + 16x + 16)$ $w_2 : (x,y) \mapsto (4/x, 8y/x^3), \quad w_{11} : (x,y) \mapsto (x, -y)$
23	$y^2 = (x^3 - x + 1)(x^3 - 8x^2 + 3x - 7)$ $w_{23} : (x,y) \mapsto (x, -y)$
26	$y^2 = x^6 - 8x^5 + 8x^4 - 18x^3 + 8x^2 - 8x + 1$ $w_{13} : (x,y) \mapsto (1/x, y/x^3), \quad w_{26} : (x,y) \mapsto (x, -y)$
28	$y^2 = (x^2 + 7)(x^2 + x + 2)(x^2 - x + 2)$ $w_4 : (x,y) \mapsto ((x+3)/(x-1), 8y/(x-1)^3), \quad w_7 : (x,y) \mapsto (x, -y), \quad w_{1/2} : (x,y) \mapsto (-x, -y)$
29	$y^2 = x^6 - 4x^5 - 12x^4 + 2x^3 + 8x^2 + 8x - 7$ $w_{29} : (x,y) \mapsto (x, -y)$
30	$y^2 = (x^2 + 4x - 1)(x^2 + x - 1)(x^4 + x^3 + 2x^2 - x + 1)$ $w_2 : (x,y) \mapsto ((x+1)/(x-1), -4y/(x-1)^4), \quad w_3 : (x,y) \mapsto (-1/x, -y/x^4),$ $w_{15} : (x,y) \mapsto (x, -y)$
31	$y^2 = (x^3 - 6x^2 - 5x - 1)(x^3 - 2x^2 - x + 3)$ $w_{31} : (x,y) \mapsto (x, -y)$
33	$y^2 = (x^2 + x + 3)(x^6 + 7x^5 + 28x^4 + 59x^3 + 84x^2 + 63x + 27)$ $w_3 : (x,y) \mapsto (3/x, -9y/x^4), \quad w_{11} : (x,y) \mapsto (x, -y)$
35	$y^2 = (x^2 + x - 1)(x^6 - 5x^5 - 9x^3 - 5x - 1)$ $w_7 : (x,y) \mapsto (-1/x, y/x^4), \quad w_{35} : (x,y) \mapsto (x, -y)$
37	$y^2 = x^6 + 14x^5 + 35x^4 + 48x^3 + 35x^2 + 14x + 1$ $w_{37} : (x,y) \mapsto (1/x, y/x^3)$
39	$y^2 = (x^4 - 7x^3 + 11x^2 - 7x + 1)(x^4 + x^3 - x^2 + x + 1)$ $w_3 : (x,y) \mapsto (1/x, y/x^4), \quad w_{39} : (x,y) \mapsto (x, -y)$
40	$y^2 = x^8 + 8x^6 - 2x^4 + 8x^2 + 1$ $w_5 : (x,y) \mapsto (-1/x, -y/x^4), \quad w_8 : (x,y) \mapsto ((1-x)/(1+x), -4y/(x+1)^4)$ $w_{1/2} : (x,y) \mapsto (-x, y)$
41	$y^2 = x^8 - 4x^7 - 8x^6 + 10x^5 + 20x^4 + 8x^3 - 15x^2 - 20x - 8$ $w_{41} : (x,y) \mapsto (x, -y)$
46	$y^2 = (x^3 + x^2 + 2x + 1)(x^3 + 4x^2 + 4x + 8)(x^6 + 5x^5 + 14x^4 + 25x^3 + 28x^2 + 20x + 8)$ $w_{23} : (x,y) \mapsto (x, -y), \quad w_{46} : (x,y) \mapsto (2/x, 8y/x^6)$
47	$y^2 = (x^5 + 4x^4 + 7x^3 + 8x^2 + 4x + 1)(x^5 - 5x^3 - 20x^2 - 24x - 19)$ $w_{47} : (x,y) \to (x, -y)$
48	$y^2 = (x^4 - 2x^3 + 2x^2 + 2x + 1)(x^4 + 2x^3 + 2x^2 - 2x + 1) = x^8 + 14x^4 + 1$ $w_{1/4} : (x,y) \to (ix, y), \quad w_3 : (x,y) \to (-1/x, -y/x^4),$ $w_{16} : (x,y) \to ((1-x)/(1+x), -4y/(1+x)^4)$
50	$y^2 = x^6 - 4x^5 - 10x^3 - 4x + 1$ $w_2 : (x,y) \mapsto (1/x, y/x^3), \quad w_{50} : (x,y) \mapsto (x, -y)$
59	$y^2 = (x^3 + 2x^2 + 1)(x^9 + 2x^8 - 4x^7 - 21x^6 - 44x^5 - 60x^4 - 61x^3 - 46x^2 - 24x - 11)$ $w_{59} : (x,y) \mapsto (x, -y)$
71	$y^2 = (x^7 - 3x^6 + 2x^5 + x^4 - 2x^3 + 2x^2 - x + 1)(x^7 - 7x^6 + 14x^5 - 11x^4 + 14x^3 - 14x^2 - x - 7)$ $w_{71} : (x,y) \mapsto (x, -y)$

Suppose that $f(x)$ has no multiple roots and denote by $\rho_1, \ldots, \rho_s \in \bar{\mathbb{Q}}$ the set of roots of f. Let $\Delta \in \mathbb{Z}$ be the discriminant of the polynomial $f(x)$. Then, the relative curve

$$\mathcal{Y} := \frac{\mathbb{Z}[\Delta^{-1}][x, y]}{\langle y^2 = f(x)\rangle} \to \mathbb{Z}[\Delta^{-1}] \tag{1}$$

is a smooth family. The set of roots $\{\rho_i\}_{i=1,\ldots,s}$ gives rise to horizontal divisors $\bar{\rho}_i$ that intersect the generic fibre of $\mathcal{Y}$ at ρ_i. The intersections of $\bar{\rho}_i$ with the fibre $\mathcal{Y}_p$ at the prime p are roots of the polynomial $f \bmod p$.

Let $\mathcal{X} \to \mathbb{Z}[(2N)^{-1}]$ be the Igusa family (with the 2-fibre removed if $2 \nmid N$). For every p such that $(p, \Delta) = 1$, the function fields of the curves $\mathcal{X}_p$ and $\mathcal{Y}_p$ have the same automorphism group.

Proof. To prove that the map given in (1) is smooth, we will show that $\mathcal{Y}_p$ is smooth for every p, so that $p \nmid \Delta$. Set $F(x) = y^2 - f(x)$. We compute

$$\frac{\partial F}{\partial y} = 2y, \quad \frac{\partial F}{\partial x} = \frac{\partial f}{\partial x}.$$

Therefore, a non-smooth point appears at $y = 0$ (since $p \neq 2$) and at a double root of $f(x) \bmod p$, that is, only at primes dividing the discriminant.

The Igusa family has good reduction at the prime 2 if $2 \nmid N$. The hyperelliptic models in Table 2 always have bad reduction at the prime 2. Therefore, the reduction of the curve $\mathcal{Y}_2$ is not related to the Igusa model. In the $2 \nmid N$ case the special fibre of the Igusa model at the prime 2 is a non-singular curve and the cover $\mathcal{X}_0(N)_2 \to \mathbb{P}^1_{\mathbb{F}_2}$ is given in terms of an Artin–Schreier extension. The automorphisms in characteristic 2 will be treated separately in Section 5.

The Igusa model is the normalization of the family $\mathcal{Y}$ at infinity at every prime in $\operatorname{Spec} \mathbb{Z}[\Delta^{-1}]$. It is known that every point P in the generic fibre $\mathcal{Y}_\eta$ defines a unique thickening, that is, a horizontal branch divisor intersecting the generic fibre at P. Since $\deg(f) \equiv 0 \bmod 2$, the place at infinity is not ramified at the cover $X_0(N) \to \mathbb{P}^1$. Therefore, the set of branch points of the cover $X_0(N) \to \mathbb{P}^1$ is contained in the generic fibre $\mathcal{Y}_\eta$ of $\mathcal{Y}$. Moreover, the thickenings $\tilde{\rho}_i$ of each point ρ_i in $\mathcal{Y}_\eta \otimes_{\mathbb{Q}} \bar{\mathbb{Q}} \subset \mathcal{X} \otimes_{\mathbb{Q}} \bar{\mathbb{Q}}$ do not intersect the singular locus of the projective closure of $\mathcal{Y}$.

The automorphism group of $\mathcal{X}_p$ is equal to the automorphism group of the corresponding function field and $\mathcal{X}_p, \mathcal{Y}_p$ share the same function field. $\qquad \square$

The automorphism group of hyperelliptic curves is a well-studied object [**5, 14, 28**]. There is the hyperelliptic involution j so that $\langle j \rangle$ is a normal subgroup of the whole automorphism group and, moreover, $X/\langle j \rangle$ is isomorphic to the projective line. The quotient $\bar{G} = \operatorname{Aut}(X)/\langle j \rangle$ is called the reduced group. The reduced group is a finite subgroup of the group of automorphisms of the projective line and these groups are given by Proposition 2.2. We introduce the following notation: for every $w \in \operatorname{Aut}(X)$, we will denote by $\bar{w}$ the image of w in the reduced group $\bar{G} := \operatorname{Aut}(X)/\langle j \rangle$.

Consider the cover $X \to X/\langle j \rangle \cong \mathbb{P}^1_k$. Let $P_1, \ldots, P_s \in \mathbb{P}^1_k$ be the branched points of the cover $X \to \mathbb{P}^1_k$. We will call the set $P_1, \ldots, P_s$ the branched hyperelliptic locus.

We know that the reduced group $\bar{G}$ induces a permutation action on them. If the points $P_1, \ldots, P_s$ are in general position, then there is no finite subgroup of $\operatorname{PGL}(2, k)$ permuting them and $\operatorname{Aut}(X) = \langle j \rangle$. The existence of additional automorphisms is a matter of special configurations of points in the configuration space of s points in the projective line. The problem of determining the primes p, so that the reduction of a hyperelliptic curve at those primes has more automorphisms, is then reduced to the problem of determining the primes at which the branch hyperelliptic locus becomes more symmetric.

We now return to the theory of hyperelliptic curves $X_0(N)$. If the number N is composite or $N = 37$, then the group of automorphisms at the generic fibre is bigger than $\mathbb{Z}/2\mathbb{Z}$. This means

that we have a non-trivial reduced group at the generic fibre. This situation gives us a lot of information for the location of fixed points of any extra automorphism in the reduction modulo p and on the possible extra automorphism groups.

For instance, the case of hyperelliptic curves that admit an extra involution was studied by Shaska and Gutierrez [**14**, **28**]. They introduced the theory of *dihedral invariants*, a theory that allows us to compute every possible extra automorphism for hyperelliptic curves of genera $2, 3$, and also gives us a lot of information in the bigger genus cases.

If the reduced automorphism group at the generic fibre is trivial, then we use a brute force method in order to compute any extra automorphism group. This is a demanding computational problem that needs several days of processing time.

Once the reduced group $\bar{G}$ of a hyperelliptic curve is determined, the group G is given in terms of an extension of groups

$$1 \to \langle j \rangle \to G \to \bar{G} \to 1.$$

For a cohomological approach to the structure of G, we refer the reader to [**17**]. It is known that the group structure of G depends on whether the fixed points of $\bar{G}$ are in the branch locus of the cover $X_0(N) \to X_0(N)^{\langle j \rangle} = \mathbb{P}_k^1$ [**5**].

PROPOSITION 2.2. *Let k be an algebraically closed field of characteristic $p \geqslant 0$. Let G be a finite subgroup of $\mathrm{Aut}(\mathbb{P}_k^1) = \mathrm{PGL}(2, k)$ and let $P_1, \ldots, P_r$ denote the number of branch points in the cover $\mathbb{P}_k^1 \to \mathbb{P}_k^1$. Denote the ramification degree of $Q \mapsto P_i$ by e_i. Then G is one of the following groups.*

(1) *Cyclic group $\mathbb{Z}/n\mathbb{Z}$ of order n relatively prime to p with $r = 2$, $e_1 = e_2 = n$.*

(2) *Elementary abelian p-group with $r = 1$, $e_1 = |G|$.*

(3) *Dihedral group D_n of order $2n$ with $p = 2$, $(p, n) = 1$, $r = 2$, $e_1 = 2$, $e_2 = n$ or $p \neq 2$, $(p, n) = 1$, $r = 3$, $e_1 = e_2 = 2$, $e_3 = n$.*

(4) *Alternating group A_4 with $p \neq 2, 3$, $r = 3$, $e_1 = 2$, $e_2 = e_3 = 3$.*

(5) *Symmetric group S_4 with $p \neq 2, 3$, $r = 3$, $e_1 = 2$, $e_2 = 3$, $e_3 = 4$.*

(6) *Alternating group A_5 with $p = 3$, $r = 2$, $e_1 = 6$, $e_2 = 5$ or $p \neq 2, 3, 5$, $r = 3$, $e_1 = 2$, $e_2 = 3$, $e_3 = 5$.*

(7) *Semidirect product of an elementary abelian p-group of order p^t with a cyclic group $\mathbb{Z}/n\mathbb{Z}$ of order n with $n|(p^t - 1)$, $r = 2$, $e_1 = |G|$, $e_2 = n$.*

(8) $\mathrm{PSL}(2, p^t)$ *with $p \neq 2$, $r = 2$, $e_1 = p^t(p^t - 1)/2$, $e_2 = (p^t + 1)/2$.*

(9) $\mathrm{PGL}(2, p^t)$ *with $r = 2$ $e_1 = p^t(p^t - 1)$, $e_2 = p^t + 1$.*

Proof. See [**33**, Theorem 1]. $\square$

REMARK 2.3. Observe that the groups $A_4, S_4, A_5, \mathrm{PSL}(2, p^t), \mathrm{PGL}(2, p^t)$ contain a dihedral group D_n, for $(n, p) = 1$.

Let $f(x)$ be a polynomial of degree s with roots $\rho_1, \ldots, \rho_s$. A simple computation shows the following.

LEMMA 2.4. *Let $A = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix} \right)$ be an invertible matrix. If $c \neq 0$ and $\rho_i c \neq a$ for all roots of f, then*

$$f\left(\frac{ax + b}{cx + d} \right) = \frac{c}{(cx + d)^s} f(a/c) \prod_{i=1}^{s} \left(x - \frac{\rho_i d - b}{-\rho_i c + a} \right). \tag{2}$$

If $c = 0$, then $\rho_i c \neq a$, since A is invertible and

$$f\left(\frac{ax + b}{d}\right) = \left(\frac{a}{d}\right)^s \prod_{i=1}^s \left(x - \frac{\rho_i d - b}{a}\right). \tag{3}$$

If there is some ρ_{i_0} such that $c\rho_i = a$, then $c \neq 0$ and

$$f\left(\frac{ax + b}{cx + d}\right) = \frac{(d\rho_{i_0} - b)}{(cx + d)^s} \prod_{i=1, i \neq i_0}^s (a - \rho_i c) \prod_{i=1, i \neq i_0}^s \left(x - \frac{\rho_i d - b}{-\rho_i c + a}\right). \tag{4}$$

DEFINITION 2.5. Let A denote the Möbius transformation $x \mapsto (ax + b)/(cx + d)$. We will denote by f_A^* the polynomial

$$f_A^*(x) := \prod_{i=1, \rho_i c \neq a}^s \left(x - \frac{\rho_i d - b}{-\rho_i c + a}\right).$$

Notice that $\deg(f) = \deg(f_A^*)$ if $c\rho_i \neq a$ for all roots ρ_i of f, or $\deg(f) = \deg(f_A^*) + 1$ if there is a root ρ_i such that $c\rho_i = a$.

LEMMA 2.6. *Let A be a Möbius transformation and set $s = \deg f$. If $s \equiv 0 \bmod 2$, then the curves $y^2 = f(x)$ and $y^2 = f_A^*(x)$ are isomorphic over a quadratic extension of $\mathbb{Q}$.*

Proof. The two curves become isomorphic under the change of variables

$$(x, y) \mapsto \left(\frac{ax + b}{cx + d}, \frac{yC^{1/2}}{(cx + d)^{s/2}}\right),$$

where C is a constant depending on which of the cases in (2), (3) or (4) we are in. $\square$

If $f(x) = \sum_{\nu=0}^s a_\nu x^n u$ is a polynomial with $a_0 \neq 0$, then we will denote by $f^*(x)$ the *reciprocal* polynomial given by $f^*(x) = a_0^{-1} x^s f(1/x) = a_0^{-1} \sum_{\nu=0}^s a_\nu x^{s-\nu}$.

If $2|s$ and $f(0) \neq 0$, then the hyperelliptic curves

$$y^2 = f(x) \text{ and } y^2 = f^*(x)$$

are isomorphic.

LEMMA 2.7. *We will denote by σ the automorphism of $\mathbb{P}_k^1$ sending x to $-x$. Consider the hyperelliptic curve*

$$X : y^2 = f(x) = \sum_{\nu=0}^s a_{2\nu} x^{2\nu}$$

that has σ in the reduced automorphism group. There is a cyclic group $\langle \sigma \rangle < C_d < \mathrm{PGL}(2, k)$ that is a subgroup of the reduced automorphism group of X if and only if $d|s$ and $a_\delta = 0$ for all $d|\delta$.

3. Curves with non-trivial reduced group

3.1. Curves of genus 2 with an extra involution

In this case we consider the set of curves $X_0(N)$ that are of genus 2 and have a reduced group isomorphic to $\mathbb{Z}/2\mathbb{Z}$. This is the case for $N = 22, 26, 28, 37, 50$.

For genus 2 curves with reduced group $\mathbb{Z}/2\mathbb{Z}$, there is a well-developed theory due to Gutierrez and Shaska [**14, 28**], namely the theory of *dihedral invariants* that reduces the

computation of the tame part of the automorphism group to the computation of several invariants of the curve.

Since $X_0(N)$ has reduced group $\mathbb{Z}/2\mathbb{Z}$, we can find a model of the curve so that the generator σ of the reduced group acts like $x \mapsto -x$. Thus, the model of our curve is of the form

$$y^2 = x^{2g+2} + a_1 x^{2g} + \ldots + a_g x^2 + 1. \tag{5}$$

The dihedral invariants are then given by $u_i := a_1^{g-i+1} a_i + a_g^{g-i+1} a_{g-i+1}$ for $i = 1, \ldots, g$. In particular, for a genus 2 curve the dihedral invariants are given by $u_1 = a_1^3 + a_2^3$, $u_2 = 2a_1 a_3$. Let V_n denote the group

$$V_n := \langle x, y \mid x^4, y^n, (xy)^2, (x^{-1}y)^2 \rangle.$$

In [**29**, Example 5.2] and [**30**], Shaska and Völklein proved that the automorphism group is isomorphic to:

(1) V_6 if and only if $(u_1, u_2) = (0, 0)$ or $(u_1, u_2) = (6750, 450)$;
(2)   (i) $\mathrm{GL}(2, 3)$ if and only if $(u_1, u_2) = (-250, 50)$ and $p \neq 5$;
     (ii) B if and only if $(u_1, u_2) = (-250, 50)$ and $p = 5$;
(3) D_6 if and only if $u_2^2 - 220u_2 - 16u_1 + 4500 = 0$;
(4) D_4 if and only if $2u_1^2 - u_2^3 = 0$ for $u_2 \neq 2, 18, 0, 50, 450$.

(Cases $0, 450, 50$ are reduced to Cases (1) and (2)). The group B mentioned above is given by

$$B := \langle a, b, c \mid c^2, a^{-5}, b^{-1}a^{-2}ba, (cb^{-1})^3, a^{-1}bca^2cac \rangle.$$

Using the exact action of the generator of the reduced group given in Table 2, we can find a model of the form (5) by diagonalizing the 2×2 matrix representing the Möbius transformation. The dihedral invariants are then computed (Table 3) and this information allows us to compute the automorphism groups given in Table 1.

3.2. Curves of genus 3 with an extra involution

A similar approach to the genus 2 in terms of the dihedral invariants can be given for the hyperelliptic curves with an involution in the reduced group that have genus 3. A complete list of all possible automorphism groups that can appear in the genus 3 case together with necessary conditions on the dihedral invariants is given in the following theorem due to Gutierrez, Sevilla and Shaska [**13**].

THEOREM 3.1. *Consider a hyperelliptic curve X of genus 3 with an extra involution. Let G denote the full automorphism group $\mathrm{Aut}(X)$ of X and $\bar{G}$ the reduced automorphism group. If the curve has $G, \bar{G}$ as in the first two columns of Table 4, then the conditions given in the third column of Table 4 are satisfied, where*

$$E_1(u_1, u_2) := 588u_2 - 5(u_3 - 8)(9u_3 - 1024),$$

$$E_2(u_1, u_2) := 7^3 u_1 - \frac{9}{8}u_3^3 - \frac{873}{2}u_3^2 + \frac{149504}{9}u_3 - \frac{1048576}{9}$$

TABLE 3. *Dihedral invariants of curves of genus 2 with extra involutions.*

N	u_1	u_2
22	$-17322/14641$	$130/121$
26	$-4351/2704$	$15/13$
28	$43625/784$	$125/7$
37	$-25642/1369$	$-198/37$
50	$-135/16$	-5

and V_8, U_6 are the groups with presentations

$$V_8 := \langle x, y \mid x^4, y^8, (xy)^2, (x^{-1}y)^2 \rangle,$$
$$U_6 := \langle x, y \mid x^2, y^{12}, xyxy^7 \rangle.$$

The curves $X_0(N)$ that are hyperelliptic of genus 3 and have an involution in the reduced group correspond to $N \in \{39, 40, 48, 33, 35, 30\}$. We compute first a hyperelliptic model of our curves so that the generator σ of an extra involution is given by $\sigma : x \mapsto -x$. These models are given in Table 5.

The dihedral invariants in the case of genus 3 curves with an extra involution are given by $u_1 = a_1^4 + a_3^4$, $u_2 = (a_1^2 + a_3^2)a_2$, $u_3 = 2a_1a_3$, where

$$y^2 = x^8 + a_1x^6 + a_2x^4 + a_3x^2 + 1$$

is a normalized model of the hyperelliptic curve. The dihedral invariants for the hyperelliptic curves $X_0(N)$ of genus 3 with an extra involution are given in Table 6.

For $N = 39$, we see that possible exceptional primes are $5, 29, 181$ and then by reducing the coefficients modulo each of these primes we see that $A(39, 5) \cong (\mathbb{Z}/2\mathbb{Z})^3$, $A(39, 29) \cong (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/4\mathbb{Z})$. The prime 181 is not exceptional. For $N = 40$, the possible exceptional primes are $3, 7$ and $A(40, 0) = (\mathbb{Z}/2\mathbb{Z}) \times D_8$ and $A(40, 3) \cong V_8$, while $A(40, 7) \cong (\mathbb{Z}/2\mathbb{Z}) \times S_4$. For $N = 48$, the possible exceptional prime is 7 and we have $A(48, 0) = (\mathbb{Z}/2\mathbb{Z}) \times S_4$, $A(48, 7) = V_8$. The full group of $\mathcal{X}_0(48)_7$ was studied by the first author in [18] and is isomorphic to an extension of $\mathrm{PGL}(2, 7)$ by $\mathbb{Z}/2\mathbb{Z}$. Using the *magma* [4] algebra system, we compute that this

TABLE 4. *Possible automorphism groups in the $g = 3$ case.*

G	$\bar{G}$	Conditions
$(\mathbb{Z}/2\mathbb{Z})^3$	$(\mathbb{Z}/2\mathbb{Z})^2$	$2u_1 - u_3 = 0$
$(\mathbb{Z}/2\mathbb{Z}) \times D_8$	D_8	$2u_1 - u_3 = 0, a_1 = a_3$
V_8	D_{16}	$2u_1 - u_3 = 0, a_1 = a_2 = a_3 = 0$
$(\mathbb{Z}/2\mathbb{Z}) \times S_4$	S_4	$(2u_1 - u_3 = 0, a_1 = a_3$ or $E_1(u_1, u_2) = E_2(u_1, u_2) = 0)$ and $((u_1, u_2, u_3) = (0, 196, 0)$ or $(81u_1, 27u_2, 8u_3) = (8192, -1280, 128))$
D_{12}	D_6	$E_1(u_1, u_2) = E_2(u_1, u_2) = 0$
$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$	D_4	$2u_1 + u_3^2 = 0$
U_6	D_{12}	$(2u_1 + u_3^2 = 0$ or $E_1(u1, u_2) = E_2(u_1, u_2) = 0)$ and $u_2 = 0$.

TABLE 5. *Models $f(x)$ for $N = 33, 35, 39, 40, 48$.*

N	$f(x)$
30	$x^8 + \frac{(276+184\sqrt{2})}{(-540\sqrt{2}-765)}x^6 - 46\,x^4 + \frac{(-184\sqrt{2}+276)}{(-540\sqrt{2}-765)}x^2 - \frac{765+540\sqrt{2}}{(-540\sqrt{2}-765)}$
33	$x^8 + \frac{(-240\sqrt{3}+508)x^6}{-264\sqrt{3}+473} + 342\,x^4 + \frac{(508+240\sqrt{3})x^2}{-264\sqrt{3}+473} + \frac{473+264\sqrt{3}}{-264\sqrt{3}+473}$
35	$5\,x^8 + (140 + 128\,i)x^6 - 34\,x^4 + (140 - 128\,i)x^2 + 5$
39	$27\,x^8 - 2^2 \cdot 97\,x^6 + 2 \cdot 29\,x^4 + 2^2 \cdot 11\,x^2 + 3$
40	$x^8 - 18x^4 + 1$
48	$x^8 + 14x^4 + 1$

group admits the following presentation:

$$A := \langle a, b, c \mid c^2, ba^{-2}b^{-1}a^{-1}, b^{-1}a^3ba^{-1}, ba^{-1}cb^{-1}a^{-1}ca^{-1}c, (a^{-1}b^{-1}cb^{-1})^2 \rangle.$$

For $N = 30, 33, 35$, the situation is a little more difficult, since the normal model is not defined over $\mathbb{Z}$ but in the principal ideal domains $\mathbb{Z}[\sqrt{2}], \mathbb{Z}[\sqrt{3}], \mathbb{Z}[i]$, respectively. We compute that the dihedral invariants in the cases $N = 33, 35$ are in $\mathbb{Q}$ and in Table 6 we present the prime factors of the numerator. For the $N = 30$ case the dihedral invariants are in $\mathbb{Q}[\sqrt{2}]$ and we compute that the principal ideals generated by the numerators of $2u_1^2 - u_g^2$ and $2u_1^2 + u_g^2$ have the prime ideals $I_2, I_{23,1}, I_{23,2}$ and $I_2, I_{23,1}, I_{23,2}, I_{17,1}, I_{17,2}$, where $I_2 = \langle 2, \sqrt{2} \rangle_{\mathbb{Z}[\sqrt{2}]}$ and $I_{23,i}, I_{17,i}$ are the prime ideals that extend the prime ideals $23\mathbb{Z}, 17\mathbb{Z}$ of the ring of rational integers. Since both conjugate prime ideals $I_{23,i}, i = 1, 2$ (respectively $I_{17,i}$) are divisors of $2u_1^2 - u_g^2$ (respectively $2u_1^2 + u_g^2$), we see that $17, 23 | (2u_1 + u_g^2)$ and $17 | (2u_1 + u_g)$. The possible exceptional primes are $p = 17, 33$. We reduce the coefficients modulo $p = 17, 33$ and we compute the automorphism group. It turns out that $A(30, 17) \cong V_8$, $A(33, 19) \cong (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/4\mathbb{Z})$, $A(33, 47) \cong (\mathbb{Z}/2\mathbb{Z})^3$.

3.3. Elementary abelian groups

The theory of dihedral invariants is working for the tame part of the automorphism group. If $p \neq 2$, then any wild part in the automorphism group will appear only in the reduced automorphism group. By looking at the table of possible subgroups of the rational function field, we see that every finite subgroup acting on the rational function field of order divisible by p should have an elementary abelian subgroup. Notice also that once one finds a prime $p \nmid N$ such that the special fibre at p contains a wild subgroup, then we can give the equation of the reduced curve and the prime p to magma and magma can compute the whole automorphism group. The difficult problem is finding the primes where the exceptional curves appear.

We will study now whether there might be an elementary abelian subgroup $E \cong (\mathbb{Z}/p\mathbb{Z})^s$ as a subgroup of the reduced group of a hyperelliptic curve. We are in the composite N case, so there is already a cyclic group inside the reduced group. For every maximal cyclic subgroup of the reduced automorphism group, we change coordinates so that the model of our curve is of the form

$$y^2 = f(x) = \sum_{\nu=0}^{s} a_{2\nu} x^{2\nu}.$$

If there is an elementary abelian group inside the reduced group modulo some prime p, then the reduced group contains $E \rtimes (\mathbb{Z}/m\mathbb{Z})$, for some m prime to p. The Galois cover $\mathbb{P}_k^1 \to \mathbb{P}_k^1$ with group $G = \mathbb{Z}_p^n \rtimes \langle \sigma \rangle$ is ramified over $0, \infty$. The elementary abelian group E fixes either 0 or ∞. If E fixes ∞, then the arbitrary $\tau \in E$ is of the form $\tau : x \mapsto x + c(\tau)$, for some $c(\tau) \in k$. In this case c is a root of all the coefficients of the polynomial $G_1(x) := f(x + c) - f(x)$ seen as a polynomial of x. If E fixes 0, then we consider the model $y^2 = f^*(x)$ of the hyperelliptic curve and now E fixes ∞. In this case, c is a root of the polynomial $G_2(x) := f^*(x + c) - f^*(x)$.

TABLE 6. *Exceptional primes for $N = 30, 33, 35, 39, 40, 48$.*

N	Factors of $2u_1 + u_g^2$	Factors of $2u_1 - u_g^2$	Possible exceptional primes	Exceptional primes
30	2, 23, 17	2, 17	23, 17	17
33	2, 19, 31, 103	2, 3, 47	19, 31, 47, 103	19, 47
35	3, 67	2, 7	3, 67	
39	2, 29, 181	2, 5, 13	5, 29, 181	5, 29
40	0	0	3	3
48	0	0	7	7

The possible primes p, so that there is an elementary abelian E group in the reduced group modulo p, are the divisors of $2g + 2$, if E does not fix any of the roots of the right-hand side of the defining equation of the hyperelliptic curve. If E fixes such a root, then $p \mid 2g + 1$, but then there are a lot of cyclic groups in the reduced group. This is the case in $A(48, 7)$ and in $A(50, 5)$.

Looking at the degrees of modular hyperelliptic curves $X_0(N)$, where N is composite we obtain that only for $p = 3$ might the reduction have some extra automorphisms. The modular hyperelliptic curves with degree divisible by 3 are those with $N \in \{22, 26, 28, 50, 46\}$. On the generic fibre, if $N \neq 28$, then the reduced group on the generic fibre is isomorphic to $\mathbb{Z}/2\mathbb{Z}$, while, for $N = 28$, the reduced group on the generic fibre is isomorphic to D_4.

We compute the polynomials $G_1(N)$ and $G_2(N)$ for every $N \in 22, 26, 28, 50, 46$ and we arrive at Table 7.

From that table we see that the curves $X_0(22)_3$, $X_0(28)_3$, $X_0(50)_3$, $X_0(46)_3$ admit an extra $\mathbb{Z}/3\mathbb{Z}$ automorphism group, while $X_0(26)_3$ does not.

3.4. The $X_0(46)$ curve

The curve $X_0(46)$ is a curve of genus 5 and has reduced automorphism group in the generic fibre isomorphic to $\mathbb{Z}/2\mathbb{Z} = \langle \sigma_1 \rangle$. We compute the following model of our curve, so that σ_1 acts like $\sigma_1 : x \mapsto -x$.

$$y^2 = x^{12} + \frac{(-4896\sqrt{2} - 6786)x^{10}}{-2392\sqrt{2} - 3381} + \frac{(-3512\sqrt{2} - 4891)x^8}{-2392\sqrt{2} - 3381} - \frac{2652x^6}{-2392\sqrt{2} - 3381}$$

$$+ \frac{(3512\sqrt{2} - 4891)x^4}{-2392\sqrt{2} - 3381} + \frac{(4896\sqrt{2} - 6786)x^2}{-2392\sqrt{2} - 3381} + \frac{-3381 + 2392\sqrt{2}}{-2392\sqrt{2} - 3381}.$$

We compute the decomposition of the coefficients of the above polynomial and we see that there is no prime P of $\mathbb{Z}[\sqrt{2}]$ with $\mathrm{Norm}(P) \neq 2, 3, 23$, so that the reduction of the curve at the prime P has a cyclic group containing σ_1.

We compute the dihedral invariants of this curve. We know that if the reduced group $\bar{G}$ contains $(\mathbb{Z}/2\mathbb{Z})^2$ as a subgroup, then $2^{g-1}u_1^2 - u_g^{g+1} = 0$ [**14**, Theorem 3.8]. The primes p such that $2^{g-1}u_1^2 - u_g^{g+1}$ becomes zero modulo p are possible primes where the reduced group can

TABLE 7. Tables of $G_1(N), G_2(N)$.

22	G_1	$(2c^3 + 2c)x^3 + (2c^3 + c)x + c^6 + 2c^4 + 2c^2$
	G_2	0
26	$G1$	$(2c^3 + c)x^3 + xc^3 + c^6 + c^4$
	G_2	$x^3c^3 + 2xc + 2c^6 + c^2$
28	G_1	$(c^3 + 2c)x^3 + (2c^3 + c)x + 2c^6 + 2c^4 + 2c^2$
	G_2	$(c^3 + 2c)x^3 + (2c^3 + c)x + 2c^6 + 2c^4 + 2c^2$
28b	G_1	$(c^3 + 2c)x^3 + (2c^3 + c)x + 2c^6 + 2c^4 + 2c^2$
	G_2	$(c^3 + 2c)x^3 + (2c^3 + c)x + 2c^6 + 2c^4 + 2c^2$
28c	G_1	$2x^3c^3 + c^6 + c^3$
	G_2	$2x^3c^3 + c^6 + c^3$
50	G_1	$(c^3 + c)x^3 + (c^3 + c)x + 2c^6 + c^4 + 2c^2$
	G_2	$(c^3 + 2c)x^3 + (2c^3 + 2c)x + 2c^6 + 2c^4 + c^2$
46	G_1	0
37	G_2	0

be large enough to contain $(\mathbb{Z}/2\mathbb{Z})^2$. We compute that

$$2^{(g-1)/2}u_1 - u_g^{(g+1)/2} = \frac{2^{23} \cdot 3^{12} \cdot 337^2 \cdot 683^2}{23^6 \cdot (-147 + 104\sqrt{2})^5(147 + 104\sqrt{2})},$$

$$2^{(g-1)/2}u_1 + u_g^{(g+1)/2} = \frac{2^{10} \cdot 3^{12} \cdot 7^2 \cdot 13^2 \cdot 281^2 \cdot 709^2}{23^6 \cdot (-147 + 104\sqrt{2})^5(147 + 104\sqrt{2})}.$$

Only the prime $p = 3$ gives rise to an extra automorphism modulo p. For this prime we have a reduced group isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ and $A(46, 3) \cong (\mathbb{Z}/2\mathbb{Z})^3$.

We will now see if there are primes so that σ_1 is the involution of a dihedral group and there is an element τ of order n so that σ_1, τ generate a dihedral group. We consider the polynomials

$$g(x) = \frac{(x+1)^{2s}}{f(-1)} f\left(\frac{1-x}{1+x}\right) = f_A^*(x), \quad \text{where } A = \begin{pmatrix} -1 & 1 \\ 1 & 1 \end{pmatrix},$$

so that σ_1 acts on the model $y^2 = g(x)$ as an involution sending $x \mapsto 1/x$. The polynomial $g(x)$ is given by

$$g(x) = g_1(x)g_2(x),$$

where

$$g_1(x) = (x^6 + 5/2\,\sqrt{2}x^5 + 5\,x^4 + \tfrac{21}{4}\,\sqrt{2}x^3 + 5\,x^2 + 5/2\,\sqrt{2}x + 1),$$
$$g_2(x) = (x^6 + 5/2\,\sqrt{2}x^5 + 7\,x^4 + \tfrac{25}{4}\,\sqrt{2}x^3 + 7\,x^2 + 5/2\,\sqrt{2}x + 1).$$

A model of a dihedral group acting on the rational function field is given by $\tau_{\text{norm}} : x \mapsto 1/(x)$ and $\sigma_{\text{norm}} : x \mapsto \zeta x$, where ζ is a primitive nth root of unity. This model is conjugate by a Möbius transformation $Q : x \mapsto (ax + b)/(cx + d)$ to any other dihedral action on the rational function field. We have normalized so that $Q\tau_{\text{norm}}Q^{-1} = \tau_{\text{norm}}$. This means that for a, b, c, d we have $b = \lambda c$, $a = \lambda d$, $d = \lambda a$ and $c = \lambda b$ for some non-zero element λ. This gives that $\lambda = \pm 1$ and therefore $a = \pm b$ and $b = \pm c$. If there is a dihedral group acting on our curve modulo p, then there should be a transformation of Q of the form $x \mapsto (ax + b)/(\pm bx + \pm a)$ such that the polynomial $g_Q^*(x)$ has the coefficients a_1, a_7, a_{11} corresponding to the monomials x, x^7, x^{11} equal to zero. Indeed, the extra automorphism should act as $x \mapsto \zeta z$ for an appropriate root of unity and moreover the polynomial $g_Q^*(x)$ should be kept invariant.

The coefficients a_1, a_7, a_{11} are polynomials of a, b and we can eliminate a by using the resultant determinant. We compute:

$$\text{Resultant}_a(a_1, a_7) = \frac{3^{12} \cdot 7^2 \cdot 23^{10} \cdot 60876058793276893^2}{2^{28}} b^{144}.$$

The reduced curve can have more automorphisms only at the primes dividing the numerator of the resultant. By reducing the hyperelliptic curve modulo all those primes and studying its automorphism group, we see that the only prime where the reduced automorphism group grows is $p = 3$. Again notice that once a prime $p \nmid N$ is fixed, finding the automorphism group of the special fibre at p can be done by magma.

4. The prime N case

If N is a prime number $N \neq 37$ so that $X_0(N)$ is hyperelliptic, then, on the generic fibre, there is only one involution, the hyperelliptic involution. In order to determine the possible primes $p \nmid N$ so that $X_0(N)_p$ has automorphism group greater than $\mathbb{Z}/2\mathbb{Z}$ we proceed as follows: suppose that the curve admits the hyperelliptic model $y^2 = f_N(x)$, where $f_N(x) \in \mathbb{Z}[x]$. We consider an arbitrary Möbius transformation σ given by $x \mapsto (ax + b)/(cx + d)$. Then we consider the

coefficients of the polynomial

$$f_N(x) - f_N\left(\frac{ax+b}{cx+d}\right)(cx+d)^{\deg f_N} = \sum_{\nu=0}^{\deg f_N} a_i x^i. \tag{6}$$

If σ is an automorphism, then all a_i should be zero. We would like to find if the system $a_i = 0$ has solutions modulo p. We consider the ideal $I_r := \langle a_i, i = 1, \ldots, r \rangle \lhd \mathbb{Z}[a, b, c, d]$, where $r < \deg f_N$. We compute a Gröbner basis for the ideal I_r with respect to the lexicographical order $a < b < d < c$, and then we form the set S of all basis elements that are polynomials in c only. Since in the generic fibre the only admissible automorphism is the trivial one, the greatest common divisor of elements in S is c^α for some $1 < \alpha \in \mathbb{N}$. We divide every element in S by c^α and we obtain an integer δ as an element in the set $\{f/c^\alpha : f \in S\}$. The prime factors p of δ are exactly the possible primes where an automorphism σ with $c \neq 0$ can appear.

We do again the same procedure, but now we choose the lexicographical order where $a < c < d < b$. We find again an integer δ' and the divisors of δ' are exactly the possible primes where an automorphism σ with $d \neq 0$ can appear.

If we select a big r, then the procedure of finding the Gröbner basis is difficult. If on the other hand we select a small r ($4 \leqslant r$, since we need at least four equations in order to find a unique solution in a, b, c, d), then we obtain big integers δ, δ' that we are not able to factorize. A selection of $r = 6$ allows us to perform the computations needed for the given set of N.

Now for each prime p that is a divisor of δ or δ' we consider the ideals $I_{\deg f_N} \otimes_{\mathbb{Z}} \mathbb{Z}/p\mathbb{Z}$ and we do the same elimination procedure. The Gröbner basis computation is easier to perform over a finite field and we finally arrive at a solution of the system $a_i = 0 \bmod p$.

For example, for the $N = 41$ case the only exceptions can happen at the primes $2, 17, 41$. The primes $2, 41$ are excluded so we focus on the $p = 17$ case. We reduce our curve modulo 17 and then we compute that the ideal $I_{\deg f_{41}} \otimes_{\mathbb{Z}} \mathbb{Z}/p\mathbb{Z}$ has a Gröbner basis of the form

$$\{a + 16d + b, d^8 + 12b^8 + 16, b(d + 8b), c + 8b, b(b^8 + 13)\}.$$

We will now solve the above system. If $b = 0$, then we see that $c = 0$ and $a = d$; therefore, we obtain the identity matrix. If $b \neq 0$, then $b^8 + 13 = 0 \Rightarrow b^4 = 2$. Let b be a fourth root of 2 in $\bar{\mathbb{F}}_{17}$. Then $c = -8b$, $d = -8b$ and $a = -9b$. The equation $d^8 + 12b^8 + 16$ is compatible with the system. Thus, we obtain the extra automorphism σ so that $\bar{\sigma} : x \mapsto (-9bx + b)/(-8bx - 9b) = (9x - 1)/(8x + 9)$. The automorphism group in this case is $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$.

There might also be an extra automorphism σ modulo p so that $b = c = 0$. Then $\sigma : x \mapsto (a/d)x$, where a/d is an nth root of unity. This does not happen for any prime p, as one easily checks. Our results are collected in Table 1.

REMARK 4.1. For the case $N = 71$, the polynomial $f_{71}(x)$ has degree 14. Then the coefficients a_i in (6) are polynomials of degree 14 in a, b, c, d. The computation of the Gröbner basis over $\mathbb{Z}$ is very time and memory consuming. For such situations, we use the following trick. If we homogenize the polynomial $f_N(x)$ into a binary form $f_N(x, y)$, then the property (6) means that $f_N(x, y)$ is invariant under the substitution $(x, y) \mapsto (ax + by, cx + dy)$. Any transvectant

$$(f_N, f_N)^r = \sum_{k=0}^{r} (-1)^k \binom{r}{k} \frac{\partial^r f_N}{\partial x^{r-k} \partial y^k} \frac{\partial^r f_N}{\partial x^k \partial y^{r-k}}$$

of $f_N(x, y)$ with itself is also invariant under this substitution (see [**10**, p. 54]). Thus, for $X_0(71)$ we first work on $g = (f_{71}, f_{71})^{10}$ of degree 8. We determine all possible primes p such that there exists non-trivial automorphisms for g modulo p. We then determine whether these primes indeed give extra automorphisms for $X_0(71)_p$.

5. *Automorphisms in characteristic* 2

In this section we will study modular hyperelliptic curves $X_0(N)$ for N odd, in characteristic 2. These curves admit a minimal Weierstrass model of the form $y^2 + q(x)y = p(x)$ [**21**] that can easily be found with the help of the *magma* algebra system. For these curves there is a notion of discriminant and for every prime not dividing the discriminant the reduction of the curve is non-singular [**21**, Theorem 1.7].

The equations are given in Table 8. These models are examples of the unified Artin–Schreier–Kummer theory in the sense of Sekiguchi and Suwa [**26, 27**]. We also observe that the discriminant of the Weierstrass equation given in Table 8 corresponding to $X_0(N)$ is N. Thus, the minimal hyperelliptic models of Table 8 and the models of Igusa are both regular smooth arithmetic surfaces over $\operatorname{Spec} \mathbb{Z}[N^{-1}]$. Since all non-singular fibres of a smooth arithmetic surface (smooth here means non-singular fibres) have genus $g \geqslant 2$, these fibres are irreducible and do not contain any exceptional divisor [**6, 20**]. Therefore, the model of Igusa and the hyperelliptic model are both minimal regular models over $\operatorname{Spec} \mathbb{Z}[N^{-1}]$ and are $\operatorname{Spec} \mathbb{Z}[N^{-1}]$-isomorphic. In particular, all fibres above primes $p \nmid N$ are isomorphic and have the same automorphism group.

LEMMA 5.1. *Let $\mathscr{C} := y^2 + q(x)y + p(x)$ be a hyperelliptic curve of genus g over $\overline{\mathbb{F}}_2$ with* $\deg q(x) \leq g+1$ *and* $\deg p(x) \leq 2g+1$. *Then every automorphism σ of $\mathscr{C}$ is of the form*

$$\sigma : (x, y) \longmapsto \left(\frac{ax+b}{cx+d}, \frac{y+h(x)}{(cx+d)^{g+1}} \right)$$

for some $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \operatorname{GL}(2, \overline{\mathbb{F}}_2)$ and $h(x) \in \overline{\mathbb{F}}_2[x]$ of degree at most $g+1$ satisfying

$$q\left(\frac{ax+b}{cx+d} \right)(cx+d)^{g+1} = q(x), \quad p\left(\frac{ax+b}{cx+d} \right)(cx+d)^{2g+2} = p(x) + h(x)^2 + q(x)h(x).$$

In particular, the hyperelliptic involution is given by

$$j(x) = x, \quad j(y) = y + q(x). \tag{7}$$

TABLE 8. *Global minimal Weierstrass equations for $X_0(N)$, N odd.*

N	Equation
23	$y^2 + (x^3 + x + 1)y = -2x^5 - 3x^2 + 2x - 2$
29	$y^2 + (x^3 + 1)y = -x^5 - 3x^4 + 2x^2 + 2x - 2$
31	$y^2 + (x^3 + x + 1)y = -2x^5 + x^4 + 4x^3 - 3x^2 - 4x - 1$
33	$y^2 + (x^4 + x^2 + 1)y = 2x^7 + 9x^6 + 27x^5 + 56x^4 + 81x^3 + 85x^2 + 54x + 20$
35	$y^2 + (x^4 + x^2 + 1)y = -x^7 - 2x^6 - x^5 - 3x^4 + x^3 - 2x^2 + x$
37	$y^2 + (x^3 + x^2 + x + 1)y = 3x^5 + 8x^4 + 11x^3 + 8x^2 + 3x$
39	$y^2 + (x^4 + x^3 + x^2 + x + 1)y = -2x^7 + 2x^5 - 7x^4 + 2x^3 - 2x$
41	$y^2 + (x^4 + x)y = -x^7 - 2x^6 + 2x^5 + 5x^4 + 2x^3 - 4x^2 - 5x - 2$
47	$y^2 + (x^5 + x^3 + 1)y = x^9 - 8x^7 - 34x^6 - 74x^5 - 106x^4 - 103x^3 - 67x^2 - 25x - 5$
59	$y^2 + (x^6 + 1)y = x^{11} - 7x^9 - 21x^8 - 38x^7 - 51x^6 - 53x^5 - 44x^4 - 30x^3 - 17x^2 - 6x - 3$
71	$y^2 + (x^7 + x^6 + x^4 + x + 1)y = -3x^{13} + 9x^{12} - 17x^{11} + 16x^{10} - 12x^9$ $+ 3x^8 + 9x^7 - 17x^6 + 16x^5 - 15x^4 + 10x^3 - 7x^2 + x - 2$

Proof. The function field of $\mathscr{C}$ is an Artin–Schreier extension of the rational function field $\overline{\mathbb{F}}_2(x)$. Indeed, if we set $Y = y/q$, then we have

$$Y^2 + Y = \frac{p}{q^2},$$

and the hyperelliptic involution is given by $(x, Y) \mapsto (x, Y + 1)$, that is, $\sigma(y) = y + q$. The hyperelliptic involution is in the center of the automorphism group. Thus, the restriction of an automorphism σ of $\mathscr{C}$ to $\overline{\mathbb{F}}_2(x)$ gives an automorphism of $\overline{\mathbb{F}}_2(x)$. Therefore, we must have $\sigma(x) = (ax + b)/(cx + d)$ for some $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ in $\mathrm{GL}(2, \overline{\mathbb{F}}_2)$.

Recall [**21**, Proposition 1.12] that a basis for the space of holomorphic differentials on $\mathscr{C}$ is given by

$$\omega_i = \frac{x^{i-1} dx}{2y + q} = \frac{x^{i-1} dx}{q}, \quad 1 \leqslant i \leqslant g,$$

and every automorphism σ of $\mathscr{C}$ induces a linear action on the space of holomorphic differentials. Write $q((ax + b)/(cx + d))(cx + d)^{g+1} = q^*(x) \in \overline{\mathbb{F}}_2[x]$. We find

$$\sigma(\omega_i) = \frac{\sigma(x)^{i-1} d\sigma(x)}{q(\sigma(x))} = (ad - bc)(ax + b)^{i-1}(cx + d)^{g-i} \frac{dx}{q^*}.$$

Since each $\sigma(\omega_i)$ is a linear combination of ω_j, we must have $q^* = \lambda q$ for some $\lambda \in \overline{\mathbb{F}}_2^*$. Because for any $\alpha \in \overline{\mathbb{F}}_2^*$, $\alpha \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ defines the same automorphism on $\overline{\mathbb{F}}_2(x)$ as $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$, we may rescale a, b, c, d so that $\lambda = 1$, that is, we have

$$q\left(\frac{ax + b}{cx + d}\right)(cx + d)^{g+1} = q(x). \tag{8}$$

We now consider $\sigma(y)$. We write it in the form $\sigma(y) = \mu y + \nu$ with $\mu, \nu \in \overline{\mathbb{F}}_2(x)$. Substituting the expression into $\sigma(y)^2 + q(\sigma(x))\sigma(y) + p(\sigma(x)) = 0$ and using (8), we obtain

$$y^2 + \frac{q(x)}{\mu(cx + d)^{g+1}} y + \frac{p(\sigma(x)) + \nu^2 + q(x)\nu/(cx + d)^{g+1}}{\mu^2} = 0.$$

Comparing this with $y^2 + q(x)y + p(x) = 0$, we find $\mu = 1/(cx + d)^{g+1}$ and $\nu(cx + d)^{g+1}$ is a polynomial $h(x)$ such that

$$p\left(\frac{ax + b}{cx + d}\right)(cx + d)^{2g+2} = p(x) + h(x)^2 + q(x)h(x).$$

This completes the proof of the lemma. $\qquad\square$

LEMMA 5.2. *Let X be a hyperelliptic curve in characteristic* 2. *The group structure of the full automorphism subgroup G of X is determined by the structure of the 2-Sylow subgroup of G.*

Proof. Let $\bar{G}$ denote the reduced group of G. By the theory of group extensions, the group G is determined uniquely by a cohomology class in the group $H^2(\bar{G}, \mathbb{Z}/2\mathbb{Z})$ corresponding to the first row of the diagram (9).

For p prime, let $H^2(\bar{G}, \mathbb{Z}/2\mathbb{Z})_p$ denote the p-part of the finite abelian group $H^2(\bar{G}, \mathbb{Z}/2\mathbb{Z})$ and let $\bar{G}_p$ denote the p-Sylow subgroup of the reduced group $\bar{G}$. Denote also the order of $\bar{G}$ by s. The following map is a monomorphism (see [**34**, p. 93]).

$$\Phi : H^2(\bar{G}, \mathbb{Z}/2\mathbb{Z}) = \bigoplus_{p|s} H^2(\bar{G}, \mathbb{Z}/2\mathbb{Z})_p \to \bigoplus_{p|s} H^2(\bar{G}_p, \mathbb{Z}/2\mathbb{Z}),$$

$$\alpha = \sum_{p|s} \alpha_p \mapsto \sum_{p|s} res_{\bar{G}, \bar{G}_p}(\alpha_p)$$

Now, if $(p, 2) = 1$, then $H^2(\bar{G}_p, \mathbb{Z}/2\mathbb{Z}) = 0$. Therefore, we have to consider only the $p = 2$ case. This proves that $H^2(\bar{G}, \mathbb{Z}/2\mathbb{Z})$ is itself a group of order a power of 2, since all p-parts of that group are mapped into 0. Moreover, the restriction map $H^2(\bar{G}, \mathbb{Z}/2\mathbb{Z}) \to H^2(\bar{G}_2, \mathbb{Z}/2\mathbb{Z})$ is a monomorphism. The class $res_{\bar{G}, \bar{G}_2}(\alpha_2)$ corresponds to the subextension given by the second row of the diagram (9).

$$
\begin{array}{ccccccccc}
1 & \longrightarrow & \mathbb{Z}/2\mathbb{Z} & \longrightarrow & G & \overset{\pi}{\longrightarrow} & \bar{G} & \longrightarrow & 1 \\
& & {\scriptstyle =}\big\downarrow\big\uparrow & & {\scriptstyle 1-1}\big\uparrow & & {\scriptstyle 1-1}\big\uparrow & & \\
1 & \longrightarrow & \mathbb{Z}/2\mathbb{Z} & \longrightarrow & G_2 & \longrightarrow & \bar{G}_2 & \longrightarrow & 1
\end{array}
\tag{9}
$$

This means that the structure of G_2 determines uniquely the structure of G. □

COROLLARY 5.3. *If $\bar{G}_2 = \{1\}$, then $G = \mathbb{Z}/2\mathbb{Z} \times \bar{G}$.*

COROLLARY 5.4. *Let $\bar{G}_2$ denote the 2-Sylow subgroup of the reduced group. This group is elementary abelian and fixes only one point ∞ of $\mathbb{P}^1$. If ∞ does not ramify in $X \to \mathbb{P}^1$, then $G = \bar{G} \times \mathbb{Z}/2\mathbb{Z}$.*

Proof. If ∞ does not ramify in $X \to \mathbb{P}^1$, then there are two points P_1, P_2 of X above ∞. The group $\langle \sigma \rangle := \mathbb{Z}/2\mathbb{Z} = \mathrm{Gal}(X/\mathbb{P}^1)$ transfers P_1 to P_2. Consider the isotropy supgroup $G_2(P_1)$. By the transitivity of the ramification index, we have that $|G_2(P_1)| = |\bar{G}_2|$. The map $G_2(P_1) \to \bar{G}_2$ is onto and, since the two groups have the same order, it is an isomorphism. Therefore, π has a section and the last line of (9) splits. The first line splits also and $G = \bar{G} \times \mathbb{Z}/2\mathbb{Z}$, since the hyperelliptic involution is central. □

The group $\bar{G}_2$ is elementary abelian and therefore it is generated by the commuting elements x_i, $i = 1, \dots, s$, that is, $\bar{G}_2 = (\mathbb{Z}/2\mathbb{Z})^s$. If the group G_2 is not a direct product, then there are elements say $\sigma \in G_2$ of order 4. Every such element when raised to the square gives the hyperelliptic involution, that is, $j = \sigma^2$. For the elements x_i such that $\pi^{-1}\langle x_i \rangle$ is a cyclic group of order 4, select a generator σ_i for this group. All these elements have squares equal to j. Order the elements x_i so that for $1 \leqslant i \leqslant \nu_0$ the group $\pi^{-1}\langle x_i \rangle$ is a cyclic group of order 4 and for $\nu_0 > 1$ the group $\pi^{-1}(\langle x_i \rangle)$ is a direct product of two cyclic groups. The group G_2 admits the following presentation in terms of generators and relations:

$$
G_2 := \left\langle j, \sigma_\nu, x_\mu : 1 \leqslant \nu \leqslant \nu_0 < \mu \; \middle| \; \begin{array}{l} \sigma_\nu^2 = j, j^2 = 1, x_\mu^2 = 1, \\ 1 = [x_\mu, x_{\mu'}] = [x_\mu, \sigma_\nu^2] = [\sigma_\nu, \sigma_{\nu'}] \end{array} \right\rangle.
$$

For every Weierstrass model given in Table 8 we use Lemma 5.1 in order to determine the automorphism group in characteristic 2. For every entry in that table we do not get any new automorphism except in the cases $N = 33, 37$.

5.1. *Case $X_0(37)$*

By Table 8, a Weierstrass model for $X_0(37)_2$ is given by $y^2 + q(x)y = p(x)$ with

$$
q(x) = x^3 + x^2 + x + 1, \quad p(x) = x^5 + x^3 + x.
$$

The hyperelliptic involution j is $j : (x, y) \mapsto (x, y + q(x))$. Let G denote the automorphism group of $X_0(37)_2$ and $\overline{G} = G/\langle j \rangle$ be the reduced automorphism group, considered as a subgroup of $\mathrm{Aut}\overline{\mathbb{F}}_2(x) = \mathrm{PGL}(2, \overline{\mathbb{F}}_2)$. According to Lemma 5.1, an element of G takes the form

$$
(x, y) \longmapsto \left(\frac{ax + b}{cx + d}, \frac{y + h(x)}{(cx + d)^3} \right),
$$

where $h(x) = u_0 + u_1 x + u_2 x^2 + u_3 x^3 \in \overline{\mathbb{F}}_2[x]$ is a polynomial of degree at most 3 and $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \overline{G} \subset \mathrm{GL}(2, \overline{\mathbb{F}}_2)$ satisfies

$$q\left(\frac{ax+b}{cx+d}\right)(cx+d)^3 = q(x), \quad p\left(\frac{ax+b}{cx+d}\right)(cx+d)^6 = p(x) + h(x)^2 + q(x)h(x).$$

These two conditions give a set of relations among a, b, c, d and u_i. The Gröbner basis of the ideal generated by these relations with respect to the lexicographic order $u_0 > u_1 > u_2 > u_3 > a > b > d > c$ is

$$u_0 + u_3 + d^2 c^4 + d^2 c + dc^8 + dc^2 + c^{192} + c^{180} + c^{168} + c^{165} + c^{150} + c^{138} + c^{135}$$
$$+ c^{132} + c^{120} + c^{105} + c^{96} + c^{90} + c^{84} + c^{75} + c^{69} + c^{66} + c^{48} + c^{36} + c^{18} + c^9,$$
$$u_1 + u_3 + d^2 c + dc^8 + c^{168} + c^{138} + c^{120} + c^{105} + c^{90} + c^{75} + c^{72} + c^{60} + c^{48}$$
$$+ c^{45} + c^{30} + c^{24} + c^{18} + c^{15} + c^{12} + c^3,$$
$$u_2 + u_3 + d^2 c^4 + dc^2 + c^{180} + c^{165} + c^{150} + c^{144} + c^{135} + c^{129} + c^{96} + c^{84} + c^{69}$$
$$+ c^{66} + c^{60} + c^{48} + c^{45} + c^{36} + c^{33} + c^{30} + c^{18} + c^{15},$$
$$u_3^2 + u_3 + d^2 c^4 + d^2 c + dc^5 + dc^2 + c^{36} + c^{33} + c^{21} + c^{18} + c^6 + c^3,$$
$$a + d + c^{16} + c,$$
$$b + c^{16},$$
$$d^3 + d^2 c + dc^2 + c^{192} + c^{144} + c^{132} + c^{129} + c^{72} + c^{48} + c^{33} + c^{24} + c^{18} + c^{12} + c^9 + 1,$$
$$d(c^{16} + c) + c^{176} + c^{161} + c^{146} + c^{131} + c^{80} + c^{65} + c^{56} + c^{41} + c^{26} + c^{20}$$
$$+ c^{17} + c^{11} + c^5 + c^2,$$
$$(c^{16} + c)(c^{192} + c^{144} + c^{132} + c^{129} + c^{96} + c^{72} + c^{66} + c^{48} + c^{36} + c^{33}$$
$$+ c^{24} + c^{18} + c^{12} + c^9 + c^6 + c^3 + 1).$$

Here the polynomial of degree 192 in c in the last element of the Gröbner basis is a product of twelve irreducible polynomials of degree 8 over $\mathbb{F}_2$. Using this basis, we find that the total number of solutions in $\overline{\mathbb{F}}_2$ is 480. (Each root of the degree 192 polynomial gives two solutions and each root of $c^{16} + c$ gives six solutions.) However, since for each root α of $x^3 + 1$ in $\mathbb{F}_4$, $(u_0, u_1, u_2, u_3, a, b, c, d)$ and $(u_0, u_1, u_2, u_3, \alpha a, \alpha b, \alpha c, \alpha d)$ give the same automorphism, we find that

$$|G| = 480/3 = 160, \quad |\overline{G}| = |G|/2 = 80.$$

We now determine the structure of the automorphism group.

We first consider the reduced automorphism group $\overline{G}$. Recall that, in general, the order of a matrix in $\mathrm{PGL}(2, \overline{\mathbb{F}}_2)$ can only be 2 or an odd integer. Moreover, the order is 1 or 2 if and only if the trace is zero. Now the relation $a + d + c^{16} + c = 0$ shows that an element $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \overline{G}$ has order 1 or 2 if and only if $c \in \mathbb{F}_{16}$. Therefore, we find that the Sylow 2-subgroup of $\overline{G}$ is an elementary abelian 2-group of order 16, and is normal in $\overline{G}$. (Again, each $c \in \mathbb{F}_{16}$ gives three solutions (a, b, c, d) but, for each root α of $x^3 + 1$ in $\overline{\mathbb{F}}_2$, (a, b, c, d) and $(\alpha a, \alpha b, \alpha c, \alpha d)$ correspond to the same reduced automorphism in $\overline{G}$.) The remaining 64 elements of $\overline{G}$ all have order 5, and $\overline{G}$ has sixteen Sylow 5-subgroups. Therefore, $\overline{G}$ is the semidirect product of an elementary abelian 2-group of order 16 by a cyclic group of order 5.

Now consider the structure of G itself. Let P be its Sylow 2-subgroup, and τ be any element of order 5. The centralizer $Z_P(\tau)$ of τ in P must satisfy $|Z_P(\tau)| \equiv |P| = 32 \bmod 5$. Thus, we have $|Z_P(\tau)| = 2$ or $|Z_P(\tau)| = 32$. The latter possibility cannot occur as it would imply that $\overline{G}$ is an abelian group. Thus, we have $|Z_P(\tau)| = 2$, that is, $Z_P(\tau) = \langle j \rangle$.

We next turn the attention to the center $Z(P)$ of the Sylow 2-subgroup P itself. Observe that $\langle \tau \rangle$ acts on $Z(P)$ by conjugation. The identity automorphism and the hyperelliptic involution are left fixed by this group action. Since $|Z_P(\tau)| = 2$, all the other orbits under this

group action have five elements. In other words, we have $|Z(P)| \equiv 2 \bmod 5$, that is, $|Z(P)| = 2$ or $|Z(P)| = 32$.

Assume $|Z(P)| = 32$. Then P is an abelian group of order 32 whose elements have order at most 4 (since $P/\langle j \rangle$ is elementary abelian). Noticing that τ acts on the set of elements of order 4 in P and that $|Z_P(\tau)| = 2$, we see that the number of elements of order 4 in P must be a multiple of 5. The only possibility is that $P \simeq (\mathbb{Z}/2\mathbb{Z})^5$. However, we can easily check that the automorphism $\sigma \in G$ given by

$$\sigma : (x, y) \longmapsto \left(\frac{(\alpha+1)x + \alpha}{\alpha x + (\alpha + 1)}, \frac{y + x^2 + x}{(\alpha x + (\alpha + 1))^3} \right)$$

is an element of order 4, where α is a root of $x^2 + x + 1$ in $\mathbb{F}_4$. Therefore, we conclude that $|Z(P)|$ cannot be 32. Instead, we have $|Z(P)| = 2$, that is, $Z(P) = \langle j \rangle$.

Now we have $|Z(P)| = 2$ and $P/Z(P)$ is elementary abelian. This means that P is one of the extraspecial groups. For order 32, there are two extraspecial groups $E_{32+} := (D_4 \times D_4)/\langle(a, a)\rangle$ and $E_{32-} := (D_4 \times Q_8)/\langle(a, b)\rangle$, where a and b denote the non-trivial elements in the centers of the dihedral group D_4 and the quaternion group Q_8, respectively. To determine which one P is isomorphic to, we consider the action of $\langle \tau \rangle$ defined by conjugation on the set S of subgroups of order 16 in P.

We claim that $\tau A \tau^{-1} \neq A$ for all $A \in S$. Assume $\tau A \tau^{-1} = A$ for some $A \in S$. The centralizer $Z_A(\tau)$ of τ in A must have only one element since $|Z_P(\tau)| = 2$ and $|Z_A(\tau)| \equiv |A| \bmod 5$. In other words, $j \notin A$, but this would imply that $P \simeq A \times \langle j \rangle$, which cannot be true for an extraspecial group. Therefore, we must have $\tau A \tau^{-1} \neq A$. It follows that for each group H of order 16, the number of subgroups of P that are isomorphic to H must be divisible by 5. Now, according to the database of small groups [12], E_{32+} has nine subgroups isomorphic to $D_4 \times (\mathbb{Z}/2\mathbb{Z})$ and six subgroups isomorphic to another group H_{16} of order 16. Therefore, we conclude that P must be isomorphic to E_{32-}, which has five subgroups isomorphic to $Q_8 \times (\mathbb{Z}/2\mathbb{Z})$ and another five subgroup isomorphic to H_{16}, and the automorphism group G is a semidirect product of E_{32-} by a cyclic group of order 5.

Of course, the conclusion above can be verified by brute force computation. However, the computation is too complicated to be presented here.

5.2. Case $X_0(33)$

The conditions given in Lemma 5.1 give rise to a system in a, b, c, d describing every element in the reduced group $\bar{G}$. The Gröbner basis of this system is computed to be

$$a^2 + ac + d^2 + dc, ab + ac + bd + dc, ad + bc + d^2 + dc + c^2, ac^4 + a + dc^4 + d,$$
$$b^2 + bd + dc + c^2, bdc + bc^2 + dc^2 + c^3, d^4 + dc^3 + c^4 + 1, d^2c + dc^2, c^5 + c.$$

This gives us the following solutions (written in matrix form):

$$\bar{G} = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \right\}.$$

Thus, the group $\bar{G}$ is isomorphic to the group $\mathrm{GL}(2, \mathbb{F}_2)$ of order 6. One 2-Sylow subgroup of $\bar{G}$ is given by the group generated by the element $\tau : x \mapsto x + 1$. The fixed point of τ is the point ∞ and, since ∞ is not ramified in the cover $X \to X^{\langle j \rangle}$, Corollary 5.4 implies $G = \bar{G} \times \langle j \rangle$.

References

1. A. ADLER, 'The Mathieu group M_{11} and the modular curve $X(11)$', *Proc. Lond. Math. Soc.* (3) 74 (1997) 1–28; MR 1416724 (97k:14021).

2. A. O. L. ATKIN and J. LEHNER, 'Hecke operators on $\Gamma_0(m)$', *Math. Ann.* 185 (1970) 134–160; MR 0268123 (42 #3022).

3. P. BENDING, A. CAMINA and R. GURALNICK, 'Automorphisms of the modular curve', *Progress in Galois theory*, Developments in Mathematics 12 (Springer, New York, 2005) 25–37; MR 2148458 (2006c:14050).

4. W. BOSMA, J. CANNON and C. PLAYOUST, 'The Magma algebra system I: The user language', *J. Symbolic Comput.* 24 (1997) 235–265.

5. R. BRANDT and H. STICHTENOTH, 'Die Automorphismengruppen hyperelliptischer Kurven', *Manuscripta Math.* 55 (1986) 83–92; MR 828412 (87m:14033).

6. T. CHINBURG, 'Minimal models of curves over Dedekind rings', *Arithmetic geometry* (eds G. Cornell and J. Silverman; Springer, New York, 1986) 309–326.

7. P. DELIGNE and D. MUMFORD, 'The irreducibility of the space of curves of given genus', *Publ. Math. Inst. Hautes Études Sci.* 36 (1969) 75–109; MR 0262240 (41 #6850).

8. N. D. ELKIES, 'The automorphism group of the modular curve $X_0(63)$', *Compositio Math.* 74 (1990) 203–208; MR 1047740 (91e:11064).

9. S. GALBRAITH, 'Equations for modular curves', PhD Thesis, St. Cross College Mathematical Institute, Oxford, 1996.

10. O. E. GLENN, 'A treatise on the theory of invariants', Project Gutenberg, http://www.gutenberg.org/etext/9933.

11. J. GONZÀLEZ ROVIRA, 'Equations of hyperelliptic modular curves', *Ann. Inst. Fourier (Grenoble)* 41 (1991) 779–795; MR 1150566 (93g:11064).

12. D. J. GREEN, 'Cohomology rings of some small p-groups', http://users.minet.uni-jena.de/cohomology/.

13. J. GUTIERREZ, D. SEVILLA and T. SHASKA, 'Hyperelliptic curves of genus 3 with prescribed automorphism group', *Computational aspects of algebraic curves*, Lecture Notes Series in Computing 13 (World Scientific, Hackensack, NJ, 2005) 109–123; MR 2182037 (2006j:14038).

14. J. GUTIERREZ and T. SHASKA, 'Hyperelliptic curves with extra involutions', *LMS J. Comput. Math* 8 (2005) 102–115 (electronic); MR 2135032 (2006b:14049).

15. J.-I. IGUSA, 'Kroneckerian model of fields of elliptic modular functions', *Amer. J. Math.* 81 (1959) 561–577; MR 0108498 (21 #7214).

16. M. A. KENKU and F. MOMOSE, 'Automorphism groups of the modular curves $X_0(N)$', *Compositio Math.* 65 (1988) 51–80; MR 930147 (88m:14015).

17. A. KONTOGEORGIS, 'The group of automorphisms of cyclic extensions of rational function fields', *J. Algebra* 216 (1999) 665–706; MR 1692965 (2000f:12005).

18. A. KONTOGEORGIS, 'The group of automorphisms of the function fields of the curve $x^n + y^m + 1 = 0$', *J. Number Theory* 72 (1998) 110–136; MR 1643304 (99f:11074).

19. H.-W. LEOPOLDT, 'Über die Automorphismengruppe des Fermatkörpers', *J. Number Theory* 56 (1996) 256–282; MR 1373551 (96k:11079).

20. S. LICHTENBAUM, 'Curves over discrete valuation rings', *Amer. J. Math.* 90 (1968) 380–403.

21. P. LOCKHART, 'On the discriminant of a hyperelliptic curve', *Trans. Amer. Math. Soc.* 342 (1994) 729–752; MR 1195511 (94f:11054).

22. A. P. OGG, 'Über die Automorphismengruppe von $X_0(N)$', *Math. Ann.* 228 (1977) 279–292; MR 0562500 (58 #27775).

23. A. P. OGG, 'Hyperelliptic modular curves', *Bull. Soc. Math. France* 102 (1974) 449–462; MR 0364259 (51 #514).

24. C. S. RAJAN, 'Automorphisms of $X(11)$ over characteristic 3 and the Mathieu group M_{11}', *J. Ramanujan Math. Soc.* 13 (1998) 63–72; MR 1626720 (99f:14027).

25. C. RITZENTHALER, 'Automorphismes des courbes modulaires $X(n)$ en caractéristique p', *Manuscripta Math.* 109 (2002) 49–62; MR 1931207 (2003g:11067).

26. T. SEKIGUCHI and N. SUWA, 'Théories de Kummer–Artin–Schreier–Witt', *C. R. Acad. Sci. Paris Sér. I Math.* 319 (1994) 105–110; MR 1288386.

27. T. SEKIGUCHI and N. SUWA, 'Théorie de Kummer–Artin–Schreier et applications', *J. Théor. Nombres Bordeaux* 7 (1995) 177–189; Les Dix-huitièmes Journées Arithmétiques (Bordeaux, 1993); MR 1413576 (98d:11139).

28. T. SHASKA, 'Computational aspects of hyperelliptic curves', *Computer mathematics*, Lecture Notes Series in Computing 10 (World Scientific, River Edge, NJ, 2003) 248–257; MR 2061839 (2005h:14073).

29. T. SHASKA, 'Determining the automorphism group of a hyperelliptic curve', *Proceedings of the 2003 International Symposium on Symbolic and Algebraic Computation* (ACM, New York, 2003) 248–254 (electronic); MR 2035219 (2005c:14037).

30. T. SHASKA and H. VÖLKLEIN, 'Elliptic subfields and automorphisms of genus 2 function fields', *Algebra, arithmetic and geometry with applications*, West Lafayette, IN, 2000 (Springer, Berlin, 2004) 703–723; MR 2037120 (2004m:14047).

31. M. SHIMURA, 'Defining equations of modular curves $X_0(N)$', *Tokyo J. Math.* 18 (1995) 443–456; MR 1363479 (96j:11085).

32. P. Tzermias, 'The group of automorphisms of the Fermat curve', *J. Number Theory* 53 (1995) 173–178; MR 1344839 (96e:11084).

33. R. C. Valentini and M. L. Madan, 'A Hauptsatz of L. E. Dickson and Artin–Schreier extensions', *J. Reine Angew. Math.* 318 (1980) 156–177; MR 579390 (82e:12030).

34. E. Weiss, *Cohomology of groups*, Pure and Applied Mathematics 34 (Academic Press, New York, 1969) MR 0263900 (41 #8499).

Aristides Kontogeorgis
Max-Planck-Institut für Mathematik
Vivatsgasse 7
53111 Bonn
Germany

and

Department of Mathematics
University of the Aegean
83200 Samos
Greece

kontogar@aegean.gr

http://myria.math.aegean.gr/
∼kontogar

Yifan Yang
Max-Planck-Institut für Mathematik
Vivatsgasse 7
53111 Bonn
Germany

and

Department of Applied Mathematics
National Chiao Tung University
Hsinchu 300
Taiwan

yfyang@math.nctu.edu.tw