On the Automorphism Groups of modular curves $X_0(N)$ in positive characteristic

Aristides Kontogeorgis $^1$  
Yifan Yang $^2$

$^1$Department of Mathematics  
University of the Aegean.

$^2$Max-Planck-Institut für Mathematik Bonn, and  
Department of Applied Mathematics  
National Chiao Tung University TAIWAN

8th Panhellenic Conference in Algebra & Number Theory
Contents

1. Automorphisms of Families of Curves
2. Modular Curves
3. Equation for Modular curves
4. Hyperelliptic Curves in Characteristic 2
5. Non hyperelliptic Curves
Let $\mathcal{X} \to S$ be a family of curves over a base scheme $S$.

For every point $P : \text{Spec} \bar{k} \to S$, we will consider the *absolute* automorphism group of the fiber $P$ to be the automorphism group $\text{Aut}_{\bar{k}}(\mathcal{X} \times_S \text{Spec} \bar{k})$ where $\bar{k}$ is the algebraic closure of $k$.

**Question:** How does the automorphism group vary along the fibers $P$?
Motivation

Let $\mathcal{X} \to S$ be a family of curves over a base scheme $S$. For every point $P : \text{Spec} k \to S$, we will consider the absolute automorphism group of the fiber $P$ to be the automorphism group $\text{Aut}_{\bar{k}}(\mathcal{X} \times_S \text{Spec} \bar{k})$ where $\bar{k}$ is the algebraic closure of $k$.

Question: How does the automorphism group vary along the fibers $P$?
Let $\mathcal{X} \to S$ be a family of curves over a base scheme $S$. For every point $P : \text{Spec} \ k \to S$, we will consider the absolute automorphism group of the fiber $P$ to be the automorphism group $\text{Aut}_{\bar{k}}(\mathcal{X} \times_S \text{Spec} \bar{k})$ where $\bar{k}$ is the algebraic closure of $k$.

Question: How does the automorphism group vary along the fibers $P$?
Fermat Curves

The Fermat Equation

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

This equation gives us a “curve” over a field $k$ by considering:

$$\mathbb{P}^1_k \ni (x_0 : y_0 : z_0) \text{ so that } x_0^{p^s+1} + y_0^{p^s+1} + z_0^{p^s+1} = 0$$

The field $k$ might be $\mathbb{Q}, \overline{\mathbb{Q}}, \mathbb{R}, \mathbb{C}, F_p, \overline{F}_p$ etc.
Fermat Curves

- **The Fermat Equation**

\[ x^{p^s+1} + y^{p^s+1} + z^{p^s+1} \]

- This equation gives us a “curve” over a field \( k \) by considering:

\[ \mathbb{P}^1_k \ni (x_0 : y_0 : z_0) \text{ so that } x_0^{p^s+1} + y_0^{p^s+1} + z_0^{p^s+1} = 0 \]

- The field \( k \) might be \( \mathbb{Q}, \overline{\mathbb{Q}}, \mathbb{R}, \mathbb{C}, \mathbb{F}_p, \overline{\mathbb{F}}_p \) etc.
Fermat Curves

- The Fermat Equation

\[ x^{p^s+1} + y^{p^s+1} + z^{p^s+1} \]

- This equation gives us a “curve” over a field \( k \) by considering:

\[ \mathbb{P}^1_k \ni (x_0 : y_0 : z_0) \text{ so that } x_0^{p^s+1} + y_0^{p^s+1} + z_0^{p^s+1} = 0 \]

- The field \( k \) might be \( \mathbb{Q}, \mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{F}_p, \overline{\mathbb{F}}_p \) etc.
Arithmetic Surfaces

\[ p = 2 \quad p = 3 \]

\[ \text{Spec} \mathbb{Z} \]

\[ \text{Generic Point} \]
Theorem (Deligne-Mumford 69)

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 $\phi : \mathcal{X} \to \mathcal{X}$.

$$\text{Aut}(\mathcal{X}_\eta) \subseteq \text{Aut}(\mathcal{X}_\rho)$$
The Fermat curve

\[ x^{p^s+1} + y^{p^s+1} + z^{p^s+1} = 0 \]

It can be seen as a smooth family over \( \text{Spec} \mathbb{Z}[\frac{1}{p^s+1}] \)

\[
\text{Aut}(X, p) = \begin{cases} 
(\mu_n \times \mu_n) \rtimes S_3 & \text{if } q \neq p \\
\text{PGU}(3, p^{2s}) & \text{if } q = p
\end{cases}
\]

Tzermias, Leopoldt, Shioda.
A special fibre $\mathcal{X}_p := \mathcal{X} \times_S S/p$ with $\text{Aut}(\mathcal{X}_p) > \text{Aut}(\mathcal{X}_\eta)$ will be called exceptional. In general we know that there are finite many exceptional fibres and it is an interesting problem to determine exactly the exceptional fibres.


- $\Gamma = \text{PSL}(2, \mathbb{Z})$
- $\Gamma(N) := \{ \sigma \in \Gamma : \sigma \equiv I_2 \mod N \}$
- $\Gamma_0(N) := \left\{ \sigma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma : c \equiv 0 \mod N \right\}$
- $Y(N) := \mathbb{H}/\Gamma(N)$, $Y_0(N) = \mathbb{H}/\Gamma_0(N)$
- $X(N) = Y(N) \cup \text{cusps}$, $X_0(N) = Y_0(N) \cup \text{cusps}$

On the Automorphism Groups of modular curves $X_0(N)$
Modular Curves

- $\Gamma = \text{PSL}(2, \mathbb{Z})$
- $\Gamma(N) := \{\sigma \in \Gamma : \sigma \equiv I_2 \mod N\}$
- $\Gamma_0(N) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma : c \equiv 0 \mod N \right\}$
- $Y(N) := \mathbb{H}/\Gamma(N)$, $Y_0(N) = \mathbb{H}/\Gamma_0(N)$
- $X(N) = Y(N) \cup \text{cusps}$, $X_0(N) = Y_0(N) \cup \text{cusps}$
Modular Curves

- $\Gamma = \text{PSL}(2, \mathbb{Z})$
- $\Gamma(N) := \{ \sigma \in \Gamma : \sigma \equiv I_2 \mod N \}$
- $\Gamma_0(N) := \left\{ \sigma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma : c \equiv 0 \mod N \right\}$
- $Y(N) := \mathbb{H}/\Gamma(N), \ Y_0(N) = \mathbb{H}/\Gamma_0(N)$
- $X(N) = Y(N) \cup \text{cusps}, \ X_0(N) = Y_0(N) \cup \text{cusps}$
Modular Curves

- $\Gamma = \text{PSL}(2, \mathbb{Z})$
- $\Gamma(N) := \{\sigma \in \Gamma : \sigma \equiv I_2 \mod N\}$
- $\Gamma_0(N) := \{\sigma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma : c \equiv 0 \mod N\}$
- $Y(N) := \mathbb{H}/\Gamma(N), \ Y_0(N) = \mathbb{H}/\Gamma_0(N)$
- $X(N) = Y(N) \cup \text{cusps}, \ X_0(N) = Y_0(N) \cup \text{cusps}$
Modular Curves

- $\Gamma = \text{PSL}(2, \mathbb{Z})$
- $\Gamma(N) := \{ \sigma \in \Gamma : \sigma \equiv I_2 \mod N \}$
- $\Gamma_0(N) := \left\{ \sigma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma : c \equiv 0 \mod N \right\}$
- $Y(N) := \mathbb{H}/\Gamma(N), \ Y_0(N) = \mathbb{H}/\Gamma_0(N)$
- $X(N) = Y(N) \cup \text{cusps}, \ X_0(N) = Y_0(N) \cup \text{cusps}$
Fundamental Domain for $X_0(30)$
Automorphisms of Modular Curves over $\mathbb{C}$

- $\text{Aut}(X(N)) = \text{PSL}(2, \mathbb{Z}/N\mathbb{Z})$, Serre, K.
- $\text{Aut}(X_0(N)) = N_{\text{Aut}(\mathbb{H})}\Gamma_0(N)/\Gamma_0(N)$ unless $N = 37, 63$ that have an extra involution, Elkies, Kenku, Momose, Ogg.
Automorphisms of Modular Curves over $\mathbb{C}$

- $\text{Aut}(X(N)) = \text{PSL}(2, \mathbb{Z}/N\mathbb{Z})$, Serre, K.
- $\text{Aut}(X_0(N)) = N_{\text{Aut}(\mathbb{H})} \Gamma_0(N)/\Gamma_0(N)$ unless $N = 37, 63$ that have an extra involution, Elkies, Kenku, Momose, Ogg.
Modular Curves

\[ \mathbb{H} \rightarrow \mathbb{H}/\Gamma_0(N) \rightarrow \mathbb{H}/\Gamma(N) \rightarrow \mathbb{P}^1_{\mathbb{C}} = \mathbb{H}/\Gamma \rightarrow \infty \]
Modular Curves

\[
\mathbb{H}/\Gamma_0(N) \quad \mathbb{H}/\Gamma(N) \quad \mathbb{P}^1 \mathbb{C} = \mathbb{H}/\Gamma
\]

Non Galois

Galois

On the Automorphism Groups of modular curves $X_0(N)$
Moduli Interpretation
Theorem (Igusa 59)

The curves $X_0(N)$ have a non-singular projective model which is defined by equations over $\mathbb{Q}$, whose reduction modulo primes $p, p \nmid N$ are also non-singular, or in a more abstract language that there is a proper smooth curve $X_0(N) \to \mathbb{Z}[1/N]$ so that for $p \in \text{Spec} \mathbb{Z}[1/N]$ the reduction $X_0(N) \times_{\text{Spec} \mathbb{Z}} \mathbb{F}_p$ is the moduli space of elliptic curves with a fixed cyclic subgroup of order $N$. 
Variation of automorphisms: $X(N)$ case

- A. Adler in 97 and C.S. Rajan in 98 proved for $X(N)$, that $X(11)_3 := X(11) \times_{\text{Spec} \mathbb{Z}} \text{Spec} \mathbb{F}_3$ has the Mathieu group $M_{11}$ as the full automorphism group.

- C. Ritzenthaler in 2003 and P. Bending, A. Carmina, R. Guralnick 2005 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 $p$ has automorphism group $\text{PGU}(3,3)$ and these are the only cases where $\text{Aut}X(q)_p > \text{Aut}X(q) \cong \text{PSL}(2, p)$. 
Variation of automorphisms: \( X(N) \) case

- A. Adler in 97 and C.S. Rajan in 98 proved for \( X(N) \), that 
  \( X(11)_3 := X(11) \times_{\text{Spec} \mathbb{Z}} \text{Spec} \mathbb{F}_3 \) has the Mathieu group \( M_{11} \) as the full automorphism group.

- C. Ritzenthaler in 2003 and P. Bending, A. Carmina, R. Guralnick 2005 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 \( p \) has automorphism group \( \text{PGU}(3, 3) \) and these are the only cases where \( \text{Aut} X(q)_p > \text{Aut} X(q) \cong \text{PSL}(2, p) \).
## Hyperelliptic modular curves

<table>
<thead>
<tr>
<th>$N$</th>
<th>Equation for Modular curves</th>
</tr>
</thead>
<tbody>
<tr>
<td>22</td>
<td>$y^2 = (x^3 + 4x^2 + 8x + 4)(x^3 + 8x^2 + 16x + 16)$</td>
</tr>
<tr>
<td>23</td>
<td>$y^2 = (x^3 - x + 1)(x^3 - 8x^2 + 3x - 7)$</td>
</tr>
<tr>
<td>26</td>
<td>$y^2 = x^6 - 8x^5 + 8x^4 - 18x^3 + 8x^2 - 8x + 1$</td>
</tr>
<tr>
<td>28</td>
<td>$y^2 = (x^2 + 7)(x^2 + x + 2)(x^2 - x + 2)$</td>
</tr>
<tr>
<td>29</td>
<td>$y^2 = x^6 - 4x^5 - 12x^4 + 2x^3 + 8x^2 + 8x - 7$</td>
</tr>
<tr>
<td>30</td>
<td>$y^2 = (x^2 + 4x - 1)(x^2 + x - 1)(x^4 + x^3 + 2x^2 - x + 1)$</td>
</tr>
<tr>
<td>31</td>
<td>$y^2 = (x^3 - 6x^2 - 5x - 1)(x^3 - 2x^2 - x + 3)$</td>
</tr>
<tr>
<td>33</td>
<td>$y^2 = (x^2 + x + 3)(x^6 + 7x^5 + 28x^4 + 59x^3 + 84x^2 + 63x + 27)$</td>
</tr>
<tr>
<td>35</td>
<td>$y^2 = (x^2 + x - 1)(x^6 - 5x^5 - 9x^3 - 5x - 1)$</td>
</tr>
<tr>
<td>37</td>
<td>$y^2 = x^6 + 14x^5 + 35x^4 + 48x^3 + 35x^2 + 14x + 1$</td>
</tr>
<tr>
<td>39</td>
<td>$y^2 = (x^4 - 7x^3 + 11x^2 - 7x + 1)(x^4 + x^3 - x^2 + x + 1)$</td>
</tr>
<tr>
<td>40</td>
<td>$y^2 = x^8 + 8x^6 - 2x^4 + 8x^2 + 1$</td>
</tr>
<tr>
<td>41</td>
<td>$y^2 = x^8 - 4x^7 - 8x^6 + 10x^5 + 20x^4 + 8x^3 - 15x^2 - 20x - 8$</td>
</tr>
<tr>
<td>46</td>
<td>$y^2 = (x^3 + x^2 + 2x + 1)(x^3 + 4x^2 + 4x + 8)(x^6 + 5x^5 + 14x^4 + 25x^3 + 28x^2 + 20x + 8)$</td>
</tr>
<tr>
<td>47</td>
<td>$y^2 = (x^5 + 4x^4 + 7x^3 + 8x^2 + 4x + 1)(x^5 - 5x^3 - 20x^2 - 24x - 19)$</td>
</tr>
<tr>
<td>48</td>
<td>$y^2 = (x^4 - 2x^3 + 2x^2 + 2x + 1)(x^4 + 2x^3 + 2x^2 - 2x + 1) = x^8 + 14x^4 + 1$</td>
</tr>
<tr>
<td>50</td>
<td>$y^2 = x^6 - 4x^5 - 10x^3 - 4x + 1$</td>
</tr>
<tr>
<td>59</td>
<td>$y^2 = (x^3 + 2x^2 + 1)(x^9 + 2x^8 - 4x^7 - 21x^6 - 44x^5 - 60x^4 - 61x^3 - 46x^2 - 24x - 11)$</td>
</tr>
</tbody>
</table>
| 71  | $y^2 = (x^7 - 3x^6 + 2x^5 + x^4 - 2x^3 + 2x^2 - x + 1)$  
 $(x^7 - 7x^6 + 14x^5 - 11x^4 + 14x^3 - 14x^2 - x - 7)$ |
Hyperelliptic modular curves

- The above list is due to M. Shimura (1995) and Galbraith (1996).
- The above models are not the Igusa models. They are singular at infinity and singular at the fibers over the prime 2.
- For the prime 2 we will seek another model (Artin-Schreier extension).
- For all fibers above $p \neq 2$ we can work with them.
Hyperelliptic modular curves

- The above list is due to M. Shimura (1995) and Galbraith (1996).
- The above models are not the Igusa models. They are singular at infinity and singular at the fibers over the prime 2.
- For the prime 2 we will seek another model (Artin-Schreier extension).
- For all fibers above $p \neq 2$ we can work with them.
The above list is due to M. Shimura (1995) and Galbraith (1996).

The above models are not the Igusa models. They are singular at infinity and singular at the fibers over the prime 2.

For the prime 2 we will seek another model (Artin-Schreier extension).

For all fibers above $p \neq 2$ we can work with them.
The above list is due to M. Shimura (1995) and Galbraith (1996).

The above models are not the Igusa models. They are singular at infinity and singular at the fibers over the prime 2.

For the prime 2 we will seek another model (Artin-Schreier extension).

For all fibers above $p \neq 2$ we can work with them.
Hyperelliptic Curves have a model of the form

\[ y^2 = \prod_{i=1}^{S} (x - \alpha_i) \]

Real Points of the above curve
Hyperelliptic Curves have a model of the form
\[ y^2 = \prod_{i=1}^{s} (x - \alpha_i) \]

Real Points of the above curve
Complex Points Hyperelliptic curves

a) Two separate copies of \( \mathbb{C} \) each with \( g + 1 \) cuts.

b) The upper copy has been turned upside down and the sides of the cuts have been glued according to the arrows.

c) The surface made compact by adding one point at infinity on each
Complex Points Hyperelliptic curves

a) Two separate copies of $\mathbb{C}$ each with $g + 1$ cuts.

b) The upper copy has been turned upside down and the sides of the cuts have been glued according to the arrows.

c) The surface made compact by adding one point at infinity on each
Complex Points Hyperelliptic curves

a) Two separate copies of \( \mathbb{C} \) each with \( g + 1 \) cuts.

b) The upper copy has been turned upside down and the sides of the cuts have been glued according to the arrows.

c) The surface made compact by adding one point at infinity on each
Automorphisms of Hyperelliptic curves $p \neq 2$

- Brandt Stichtenoth 1986

  - $j : x \mapsto x, y \mapsto -y$.
  - $\mathbb{Z}/2\mathbb{Z} \cong \langle j \rangle \triangleleft \text{Aut}(C)$
  - $H := \text{Aut}(C)/\langle j \rangle$ is a finite subgroup of $\text{PGL}(2, k) = \text{Aut}(\mathbb{P}^1_k)$.
  - Problem of group extensions

$$1 \rightarrow \langle j \rangle \rightarrow \text{Aut}(C) \rightarrow H \rightarrow 1.$$ 

The structure of the group $\text{Aut}(C)$ depends on the intersection of the branch locus of the cover $\mathbb{P}^1_k \rightarrow \mathbb{P}^1_k/H$ with the set of roots $\alpha_i$. 
Brandt-Stichtenoth 1986

\[ j : x \mapsto x, \quad y \mapsto -y. \]

\[ \mathbb{Z}/2\mathbb{Z} \cong \langle j \rangle \triangleleft \text{Aut}(C) \]

\[ H := \text{Aut}(C)/\langle j \rangle \text{ is a finite subgroup of } \text{PGL}(2, k) = \text{Aut}(\mathbb{P}^1_k). \]

Problem of group extensions

\[ 1 \to \langle j \rangle \to \text{Aut}(C) \to H \to 1. \]

The structure of the group \( \text{Aut}(C) \) depends on the intersection of the branch locus of the cover \( \mathbb{P}^1_k \to \mathbb{P}^1_k/H \) with the set of roots \( \alpha_i \).
Automorphisms of Hyperelliptic curves $p \neq 2$

- Brandt Stichtenothen 1986
- $j : x \mapsto x, y \mapsto -y$.
- $\mathbb{Z}/2\mathbb{Z} \cong \langle j \rangle \triangleleft \text{Aut}(C)$
- $H := \text{Aut}(C)/\langle j \rangle$ is a finite subgroup of $\text{PGL}(2, k) = \text{Aut}(\mathbb{P}^1_k)$.
- Problem of group extensions

$$1 \rightarrow \langle j \rangle \rightarrow \text{Aut}(C) \rightarrow H \rightarrow 1.$$

The structure of the group $\text{Aut}(C)$ depends on the intersection of the branch locus of the cover $\mathbb{P}^1_k \rightarrow \mathbb{P}^1_k/H$ with the set of roots $\alpha_i$. 
Brandt Stichtenoth 1986

\[ j : x \mapsto x, \ y \mapsto -y. \]

\[ \mathbb{Z}/2\mathbb{Z} \cong \langle j \rangle \triangleleft \text{Aut}(C) \]

\[ H := \text{Aut}(C)/\langle j \rangle \text{ is a finite subgroup of } \text{PGL}(2, k) = \text{Aut}(\mathbb{P}^1_k). \]

Problem of group extensions

\[ 1 \to \langle j \rangle \to \text{Aut}(C) \to H \to 1. \]

The structure of the group Aut(C) depends on the intersection of the branch locus of the cover \( \mathbb{P}^1_k \to \mathbb{P}^1_k/H \) with the set of roots \( \alpha_i \).
Automorphisms of Hyperelliptic curves $p \neq 2$

- Brandt Stichtenoth 1986
- $j : x \mapsto x, y \mapsto -y$
- $\mathbb{Z}/2\mathbb{Z} \cong \langle j \rangle \triangleleft \text{Aut}(C)$
- $H := \text{Aut}(C)/\langle j \rangle$ is a finite subgroup of $\text{PGL}(2, k) = \text{Aut}(\mathbb{P}^1_k)$.
- Problem of group extensions

$$1 \to \langle j \rangle \to \text{Aut}(C) \to H \to 1.$$

The structure of the group $\text{Aut}(C)$ depends on the intersection of the branch locus of the cover $\mathbb{P}^1_k \to \mathbb{P}^1_k/H$ with the set of roots $\alpha_i$. 
Finite subgroups of $\text{PGL}(2, k)$

1. Cyclic group $C_n$ of order $n$ $(n, p) = 1$ 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 $C_n$ of order $n$ with $n \mid p^t - 1$, $r = 2$, $e_1 = |G|$, $e_2 = n$.
8. $\text{PSL}(2, p^t)$ with $p \neq 2$, $r = 2$, $e_1 = \frac{p^t(p^t-1)}{2}$, $e_2 = \frac{p^t+1}{2}$.
9. $\text{PGL}(2, p^t)$ with $p \neq 2$, $r = 2$, $e_1 = \frac{t(t+1)}{2}$, $e_2 = \frac{t+1}{2}$.
Platonic Solids

- Tetrahedron
  - Group: $A_4$
- Octahedron, Cube
  - Group: $S_4$
- Dodecahedron, Icosahedron
  - Group: $A_5$
Computation of $H$

- The group $H$ is determined by the configuration of the roots $\alpha_1, \ldots, \alpha_{2g+2}$ in $\mathbb{P}^1_k$.
- It can be that modulo $p$ the configuration of the roots is more symmetrical.
- The hyperelliptic curve $y^2 = x^6 + 5x^3 + 1$ is acted on by $j$ and by $\sigma : x \mapsto \zeta_3 x$.
- This curve modulo 5 is acted on by a bigger group generated by $\sigma' : x \mapsto \zeta_6 x$. 
Computation of $H$

- The group $H$ is determined by the configuration of the roots $\alpha_1, \ldots, \alpha_{2g+2}$ in $\mathbb{P}^1_k$.
- It can be that modulo $p$ the configuration of the roots is more symmetrical.
- The hyperelliptic curve $y^2 = x^6 + 5x^3 + 1$ is acted on by $j$ and by $\sigma : x \mapsto \zeta_3 x$.
- This curve modulo 5 is acted on by a bigger group generated by $\sigma' : x \mapsto \zeta_6 x$. 
The group $H$ is determined by the configuration of the roots $\alpha_1, \ldots, \alpha_{2g+2}$ in $\mathbb{P}^1_k$.

It can be that modulo $p$ the configuration of the roots is more symmetrical.

The hyperelliptic curve $y^2 = x^6 + 5x^3 + 1$ is acted on by $j$ and by $\sigma : x \mapsto \zeta_3 x$.

This curve modulo 5 is acted on by a bigger group generated by $\sigma' : x \mapsto \zeta_6 x$. 
The group $H$ is determined by the configuration of the roots $\alpha_1, \ldots, \alpha_{2g+2}$ in $\mathbb{P}^1_k$.

- It can be that modulo $p$ the configuration of the roots is more symmetrical.
- The hyperelliptic curve $y^2 = x^6 + 5x^3 + 1$ is acted on by $j$ and by $\sigma : x \mapsto \zeta_3 x$.
- This curve modulo 5 is acted on by a bigger group generated by $\sigma' : x \mapsto \zeta_6 x$. 

On the Automorphism Groups of modular curves $X_0(N)$
Vollklein, Shaska, Shevilla, Guttierez 2002-2007 developed the theory of *dihedral invariants* for hyperelliptic curves provided that $H$ has at least one involution. They also gave a classification of automorphisms depending on these invariants.

This idea is applicable to hyperelliptic curves of the form: $X_0(N)$ for $N = 22, 26, 28, 37, 50$ that are of genus 2 and for $N = 39, 40, 48, 33, 35, 30$ of genus 3.
Vollklein, Shaska, Shevilla, Guttierez 2002-2007 developed the theory of *dihedral invariants* for hyperelliptic curves provided that $H$ has at least one involution. They also gave a classification of automorphisms depending on these invariants.

This idea is applicable to hyperelliptic curves of the form: $X_0(N)$ for $N = 22, 26, 28, 37, 50$ that are of genus 2 and for $N = 39, 40, 48, 33, 35, 30$ of genus 3.
Dihedral Invariants

- Change the model so that the extra involution acts like $x \mapsto -x$ (Diagonalization).

$$y^2 = x^{2g+2} + a_1 x^{2g} + \cdots + a_g x^2 + 1.$$  

- Compute invariants $u_i := a_i^{g-i+1} a_i + a_g^{g-i+1} a_{g-i+1}$ for $i = 1, \ldots, g$
Dihedral Invariants

- Change the model so that the extra involution acts like $x \mapsto -x$ (Diagonalization).

$$y^2 = x^{2g+2} + a_1 x^{2g} + \cdots + a_g x^2 + 1.$$  

- Compute invariants $u_i := a_1^{g-i+1} a_i + a_g^{g-i+1} a_{g-i+1}$ for $i = 1, \ldots, g$
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. $\text{GL}_2(3)$ if and only if $(u_1, u_2) = (-250, 50)$ and $p \neq 5$
3. $B$ if and only if $(u_1, u_2) = (-250, 50)$ and $p = 5$
4. $D_6$ if and only if $u_2^2 - 220u_2 - 16u_1 + 4500 = 0,$
5. $D_4$ if and only if $2u_1^2 - u_2^3$ for $u_2 \neq 2, 18, 0, 50, 450.$

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

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

$$ V_n := \langle x, y | x^4, y^n, (xy)^2, (x^{-1}y)^2 \rangle. $$
A similar theorem holds. Too complicated to write it down!

An additional difficulty: The normalized models are defined over a PID different than \( \mathbb{Z} \).

<table>
<thead>
<tr>
<th>( N )</th>
<th>( f(x) )</th>
</tr>
</thead>
<tbody>
<tr>
<td>30</td>
<td>( 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)} )</td>
</tr>
<tr>
<td>33</td>
<td>( x^8 + \frac{-264 \sqrt{3}+473}{(-264 \sqrt{3}+473)} x^6 + 342 x^4 + \frac{508+240 \sqrt{3}}{(-264 \sqrt{3}+473)} x^2 + \frac{473+264 \sqrt{3}}{-264 \sqrt{3}+473} )</td>
</tr>
<tr>
<td>35</td>
<td>( 5 x^8 + (140 + 128 i) x^6 - 34 x^4 + (140 - 128 i) x^2 + 5 )</td>
</tr>
<tr>
<td>39</td>
<td>( 27 x^8 - 2^2 \cdot 97 x^6 + 2 \cdot 29 x^4 + 2^2 \cdot 11 x^2 + 3 )</td>
</tr>
<tr>
<td>40</td>
<td>( x^8 - 18 x^4 + 1 )</td>
</tr>
<tr>
<td>48</td>
<td>( x^8 + 14 x^4 + 1 )</td>
</tr>
</tbody>
</table>
A similar theorem holds. Too complicated to write it down!

An additional difficulty: The \textit{normalized} models are defined over a PID different than $\mathbb{Z}$.

<table>
<thead>
<tr>
<th>$N$</th>
<th>$f(x)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>30</td>
<td>$x^8 + \left(\frac{276 + 184\sqrt{2}}{-540\sqrt{2} - 765}\right)x^6 - 46x^4 + \left(\frac{-184\sqrt{2} + 276}{-540\sqrt{2} - 765}\right)x^2 - \frac{765 + 540\sqrt{2}}{-540\sqrt{2} - 765}$</td>
</tr>
<tr>
<td>33</td>
<td>$x^8 + \left(\frac{-264\sqrt{3} + 508}{-240\sqrt{3} + 508}\right)x^6 + 342x^4 + \frac{508 + 240\sqrt{3}}{508 + 240\sqrt{3}}x^2 + \frac{473 + 264\sqrt{3}}{-264\sqrt{3} + 473}$</td>
</tr>
<tr>
<td>35</td>
<td>$5x^8 + (140 + 128i)x^6 - 34x^4 + (140 - 128i)x^2 + 5$</td>
</tr>
<tr>
<td>39</td>
<td>$27x^8 - 2^2 \cdot 97x^6 + 2 \cdot 29x^4 + 2^2 \cdot 11x^2 + 3$</td>
</tr>
<tr>
<td>40</td>
<td>$x^8 - 18x^4 + 1$</td>
</tr>
<tr>
<td>48</td>
<td>$x^8 + 14x^4 + 1$</td>
</tr>
</tbody>
</table>
Example: $X_0(48)$

- **Generic automorphism group:** $\mathbb{Z}/2\mathbb{Z} \times S_4$.
- Possible exceptional prime $p = 7$.
- Automorphism group of the fibre at $p = 7$ to an extension of $\text{PGL}(2, 7)$ by $\mathbb{Z}/2\mathbb{Z}$. Using magma we compute that this group admits the following presentation:

$$A := \langle a, b, c \mid c^2, ba^{-2}b^{-1}a^{-1}, b^{-1}a^3b^{-1}a^{-1}, ba^{-1}cb^{-1}a^{-1}ca^{-1}c, (a^{-1}b^{-1}cb^{-1})^2 \rangle.$$
Example: $X_0(48)$

- **Generic automorphism group**: $\mathbb{Z}/2\mathbb{Z} \times S_4$.
- **Possible exceptional prime** $p = 7$.
- **Automorphism group of the fibre at** $p = 7$ to an extension of $\text{PGL}(2, 7)$ by $\mathbb{Z}/2\mathbb{Z}$. Using magma we compute that this group admits the following presentation:

$$A := \langle a, b, c \mid c^2, ba^{-2}b^{-1}a^{-1}, b^{-1}a^3ba^{-1}, ba^{-1}cb^{-1}a^{-1}ca^{-1}c, (a^{-1}b^{-1}cb^{-1})^2 \rangle.$$
Example: $X_0(48)$

- Generic automorphism group: $\mathbb{Z}/2\mathbb{Z} \times S_4$.
- Possible exceptional prime $p = 7$.
- Automorphism group of the fibre at $p = 7$ to an extension of $\text{PGL}(2, 7)$ by $\mathbb{Z}/2\mathbb{Z}$. Using magma we compute that this group admits the following presentation:

$$A := \left\langle a, b, c \mid c^2, ba^{-2}b^{-1}a^{-1}, b^{-1}a^3ba^{-1}, ba^{-1}cb^{-1}a^{-1}ca^{-1}c, (a^{-1}b^{-1}cb^{-1})^2 \right\rangle.$$
The prime $N \neq 37$ case

- These curves have only one involution the hyperelliptic one. The reduced group is not zero and the method of dihedral invariants is not applicable.

- Brute Force!
The prime $N \neq 37$ case

- These curves have only one involution the hyperelliptic one. The reduced group is not zero and the method of dihedral invariants is not applicable.
- Brute Force!
The method

- $y^2 = f_N(x)$ where $f_N(x) \in \mathbb{Z}[x]$.
- Find $\sigma$ given by $x \mapsto \frac{ax+b}{cx+d}$.
- Consider the coefficients of the polynomial

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

If $\sigma$ is an automorphism then all $a_i$ should be zero.
- Find the $p$ so that the Diophantine equations $a_i = 0$ have solutions modulo $p$. 
The method

- \( y^2 = f_N(x) \) where \( f_N(x) \in \mathbb{Z}[x] \).
- Find \( \sigma \) given by \( x \mapsto \frac{ax+b}{cx+d} \).
- Consider the coefficients of the polynomial

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

If \( \sigma \) is an automorphism then all \( a_i \) should be zero.

- Find the \( p \) so that the Diophantine equations \( a_i = 0 \) have solutions modulo \( p \).
The method

- \( y^2 = f_N(x) \) where \( f_N(x) \in \mathbb{Z}[x] \).
- Find \( \sigma \) given by \( x \mapsto \frac{ax+b}{cx+d} \).
- Consider the coefficients of the polynomial

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

If \( \sigma \) is an automorphism then all \( a_i \) should be zero.

- Find the \( p \) so that the Diophantine equations \( a_i = 0 \) have solutions modulo \( p \).
The method

- $y^2 = f_N(x)$ where $f_N(x) \in \mathbb{Z}[x]$.
- Find $\sigma$ given by $x \mapsto \frac{ax + b}{cx + d}$.
- Consider the coefficients of the polynomial

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

If $\sigma$ is an automorphism then all $a_i$ should be zero.

- Find the $p$ so that the Diophantine equations $a_i = 0$ have solutions modulo $p$. 
Consider the ideal $I_r := \langle a_i, i = 1, \ldots, r \rangle \triangleleft \mathbb{Z}[a, b, c, d]$ where $r < \deg f_N$.

Compute a Gröbner basis for $I_r$ with respect of the lex order $a < b < d < c$, and then we form the set $S$ of all basis elements that are polynomials in $c$ only.

The generic fibre the only admissible automorphism is the trivial one, the gcd of elements in $S$ is $c^\alpha$ for some $1 < \alpha \in \mathbb{N}$. We divide every element in $S$ by $c^\alpha$ and we obtain an integer $\delta$ as an element in the set $\{f/c^\alpha : f \in S\}$. The prime factors $p$ of $\delta$ are exactly the possible primes where an automorphism $\sigma$ with $c \neq 0$ can appear.

Consider the same system modulo $\overline{\mathbb{F}}_p$.
Consider the ideal $I_r := \langle a_i, i = 1, \ldots, r \rangle \triangleleft \mathbb{Z}[a, b, c, d]$ where $r < \deg f_N$.

Compute a Gröbner basis for $I_r$ with respect of the lex order $a < b < d < c$, and then we form the set $S$ of all basis elements that are polynomials in $c$ only.

The generic fibre the only admissible automorphism is the trivial one, the gcd of elements in $S$ is $c^\alpha$ for some $1 < \alpha \in \mathbb{N}$. We divide every element in $S$ by $c^\alpha$ and we obtain an integer $\delta$ as an element in the set $\{f/c^\alpha : f \in S\}$. The prime factors $p$ of $\delta$ are exactly the possible primes where an automorphism $\sigma$ with $c \neq 0$ can appear.

Consider the same system modulo $\bar{F}_p$. 

Gröbner Bases
Consider the ideal \( I_r := \langle a_i, i = 1, \ldots, r \rangle \triangleleft \mathbb{Z}[a, b, c, d] \) where \( r < \deg f_N \).

Compute a Gröbner basis for \( I_r \) with respect of the lex order \( a < b < d < c \), and then we form the set \( S \) of all basis elements that are polynomials in \( c \) only.

The generic fibre the only admissible automorphism is the trivial one, the gcd of elements in \( S \) is \( c^\alpha \) for some \( 1 < \alpha \in \mathbb{N} \). We divide every element in \( S \) by \( c^\alpha \) and we obtain an integer \( \delta \) as an element in the set \( \{ f/c^\alpha : f \in S \} \). The prime factors \( p \) of \( \delta \) are exactly the possible primes where an automorphism \( \sigma \) with \( c \neq 0 \) can appear.

Consider the same system modulo \( \overline{\mathbb{F}}_p \).
Consider the ideal \( I_r := \langle a_i, i = 1, \ldots, r \rangle \triangleleft \mathbb{Z}[a, b, c, d] \) where \( r < \deg f_N \).

Compute a Gröbner basis for \( I_r \) with respect of the lex order \( a < b < d < c \), and then we form the set \( S \) of all basis elements that are polynomials in \( c \) only.

The generic fibre the only admissible automorphism is the trivial one, the gcd of elements in \( S \) is \( c^\alpha \) for some \( 1 < \alpha \in \mathbb{N} \). We divide every element in \( S \) by \( c^\alpha \) and we obtain an integer \( \delta \) as an element in the set \( \{ f/c^\alpha : f \in S \} \). The prime factors \( p \) of \( \delta \) are exactly the possible primes where an automorphism \( \sigma \) with \( c \neq 0 \) can appear.

Consider the same system modulo \( \overline{\mathbb{F}_p} \).
Example: $N = 41$

\[ a^2 + 3d^18 - 4d^2 + 19c^18 + 15c^10 + 866c^2, \]
\[ a^2 + d^2, \]
\[ 2a + 2b^d - 7c + 2d^9 + d^7c^2 - 4d + 39c^17 + 24c^9 + 142c, \]
\[ b^8 + 3b^2d^6 + 2d^7c + d^6c^2 + 13c^24 + 22c^16 + 521c^8, \]
\[ 2b^4 + 2b^6d - 3 + 2b^2d - 2c + 2d^3c + d^2c^2 + 14c^20 + 17c^12 + 685c^4, \]
\[ 2b^2c + 2b^2d + c + 34c^19 + 12c^11 + 40c^3, \]
\[ b^2c + 2d^2c + d^2 + 39c^19 + 19c^11 + 553c^3, \]
\[ 4b + d^7c^2 + 25c^17 + 39c^9 + 1472c, \]
\[ d^24 + 40c^24 + 34c^16 + 139c^8 - 1, \]
\[ d^8c^2 + 20c^18 + 18c^10 + 199c^2, \]
\[ 2c^8d + 40c^17 + 136c^9 + 398c, \]
\[ 4c^8 + 5c^24 + 14c^16 + 677c^8 - 4, \]
\[ d^2c^2 + 16c^20 + 7c^12 + 599c^4, \]
\[ 2d^2c + 32c^19 + 14c^11 + 501c^3, \]
\[ 4d^2c + 23c^18 + 28c^10 + 264c^2, \]
\[ c^25 + 36c^17 + 39c^9 + 496c, \]
\[ 41c^9 + 2624c, \]
\[ 697c^3, \]
\[ 1394c^2, \]
\[ 2788c \]
Example: $N = 41$

- 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 to 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 $\overline{F}_{17}$. Then $c = -8b$, $d = -8b$, $a = -9b$. The equation $d^8 + 12b^8 + 16$ is compatible with the system. Thus we obtain the extra automorphism $\sigma$ so that $\sigma : x \mapsto \frac{-9bx + b}{-8bx - 9b} = \frac{9x - 1}{8x + 9}$. The automorphism group in this case is $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.  

On the Automorphism Groups of modular curves $X_0(N)$
Example: $N = 41$

- 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 to 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 $\overline{\mathbb{F}}_{17}$. Then $c = -8b$, $d = -8b$, $a = -9b$. The equation $d^8 + 12b^8 + 16$ is compatible with the system. Thus we obtain the extra automorphism $\sigma$ so that $\overline{\sigma} : x \mapsto \frac{-9bx + b}{-8bx - 9b} = \frac{9x - 1}{8x + 9}$.

The automorphism group in this case is $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. 
Example: $N = 41$

- 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 to the $p = 17$ case. We reduce our curve modulo 17 and then we compute that the ideal $I_{\deg f_{41}} \otimes \mathbb{Z}/p\mathbb{Z}$ 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 $b^8 + 13 = 0 \implies b^4 = 2$. Let $b$ be a fourth root of 2 in $\overline{F}_{17}$. Then $c = -8b$, $d = -8b$, $a = -9b$. The equation $d^8 + 12b^8 + 16$ is compatible with the system. Thus we obtain the extra automorphism $\sigma$ so that $\bar{\sigma}: x \mapsto \frac{-9bx+b}{-8bx-9b} = \frac{9x-1}{8x+9}$. The automorphism group in this case is $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. 

Minimal Weierstrass Models

- Every hyperelliptic curve of genus $g$ has a model:

$$C := y^2 + q(x)y + p(x)$$

with $\deg q(x) \leq g + 1$ and $\deg p(x) \leq 2g + 1$. (Application of Riemann-Roch theorem, Lockhart 1994)

- In characteristic $p \neq 2$ we can find a model of the form $y^2 = f(x)$ by completing the square in the left hand side.

- In characteristic 2 this model is given in terms of an Artin-Schreier extension. Set $Y = y/q$ in order to obtain

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

and the hyperelliptic involution is given by

$$(x, Y) \mapsto (x, Y + 1).$$
Every hyperelliptic curve of genus $g$ has a model:

$$C := y^2 + q(x)y + p(x)$$

with $\deg q(x) \leq g + 1$ and $\deg p(x) \leq 2g + 1$. (Application of Riemann-Roch theorem, Lockhart 1994)

In characteristic $p \neq 2$ we can find a model of the form $y^2 = f(x)$ by completing the square in the left hand side.

In characteristic 2 this model is given in terms of an Artin-Schreier extension. Set $Y = y/q$ in order to obtain

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

and the hyperelliptic involution is given by $(x, Y) \mapsto (x, Y + 1)$. 
Every hyperelliptic curve of genus \( g \) has a model:

\[
C := y^2 + q(x)y + p(x)
\]

with \( \deg q(x) \leq g + 1 \) and \( \deg p(x) \leq 2g + 1 \). (Application of Riemann-Roch theorem, Lockhart 1994)

In characteristic \( p \neq 2 \) we can find a model of the form \( y^2 = f(x) \) by completing the square in the left hand side.

In characteristic 2 this model is given in terms of an Artin-Schreier extension. Set \( Y = y/q \) in order to obtain

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

and the hyperelliptic involution is given by \((x, Y) \mapsto (x, Y + 1)\).
Every hyperelliptic curve of genus $g$ has a model:

$$C := y^2 + q(x)y + p(x)$$

with $\deg q(x) \leq g + 1$ and $\deg p(x) \leq 2g + 1$. (Application of Riemann-Roch theorem, Lockhart 1994)

In characteristic $p \neq 2$ we can find a model of the form $y^2 = f(x)$ by completing the square in the left hand side.

In characteristic 2 this model is given in terms of an Artin-Schreier extension. Set $Y = y/q$ in order to obtain

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

and the hyperelliptic involution is given by

$$(x, Y) \mapsto (x, Y + 1).$$
A basis for the space of holomorphic differentials on $C$ is given by

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

Every automorphism $\sigma$ of $C$ induces a linear action on the space of holomorphic differentials.

Write $q((ax + b)/(cx + d))(cx + d)^{g+1} = q^*(x) \in \overline{F}_2[x]$.

$q^* = \lambda q$
A basis for the space of holomorphic differentials on $C$ is given by

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

Every automorphism $\sigma$ of $C$ induces a linear action on the space of holomorphic differentials.

Write $q((ax + b)/(cx + d))(cx + d)^{g+1} = q^*(x) \in \overline{F}_2[x]$.

$q^* = \lambda q$
A basis for the space of holomorphic differentials on $C$ is given by

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

Every automorphism $\sigma$ of $C$ induces a linear action on the space of holomorphic differentials.

Write $q((ax + b)/(cx + d))(cx + d)^{g+1} = q^*(x) \in \overline{F}_2[x]$.

$q^* = \lambda q$
A basis for the space of holomorphic differentials on $C$ is given by

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

Every automorphism $\sigma$ of $C$ induces a linear action on the space of holomorphic differentials.

Write $q((ax + b)/(cx + d))(cx + d)^{g+1} = q^*(x) \in \overline{F}_2[x]$.

$q^* = \lambda q$
Theorem

Let $C := y^2 + q(x)y + p(x)$ 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 $\sigma$ of $C$ is of the form

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

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

$$q \left( \frac{ax + b}{cx + d} \right) (cx + d)^{g+1} = q(x), \quad p \left( \frac{ax + b}{cx + d} \right) (cx + d)^{2g+2} = p(x) + h(x)^2 + q(x)h(x).$$
Example: $X_0(37)$ in characteristic 2

- Weierstrass model:

$$y^2 + (x^3 + x^2 + x+)y = x^5 + x^3 + x$$

- Search for $a, b, c, d$ so that the conditions of the previous theorem is fulfilled. System of equations, Gröbner basis approach.
Example: $X_0(37)$ in characteristic 2

- Weierstrass model:

  $$y^2 + (x^3 + x^2 + x+)y = x^5 + x^3 + x$$

- Search for $a, b, c, d$ so that the conditions of the previous theorem is fulfilled. System of equations, Gröbner basis approach.
Example: \(X_0(37)\) in characteristic 2

- Gröbner basis.

\[
\begin{align*}
u_0 + u_3 + d^2 c^4 + d^2 c + dc^8 + dc^2 + c^{192} + c^{180} + c^{168} + c^{165} + c^{150} + c^{138} + c^{135} + c^{132} + c^{120} + c^{105} + c^96 + c^90 + c^84 + c^75 + c^69 + c^66 + c^48 + c^36 + c^18 + c^9, \\
u_1 + u_3 + d^2 c + dc^8 + c^{168} + c^{138} + c^{120} + c^{105} + c^90 + c^75 + c^72 + c^60 + c^{48} + c^{45} + c^{30} + c^{24} + c^{18} + c^{15} + c^{12} + c^9, \\
u_2 + u_3 + d^2 c + dc^2 + c^{180} + c^{165} + c^{150} + c^{144} + c^{135} + c^{129} + c^96 + c^84 + c^69 + c^{60} + c^{48} + c^{45} + c^{36} + c^{33} + c^{30} + c^{18} + c^{15}, \\
u_3 + u_3 + d^2 c^4 + d^2 c + dc^5 + dc^2 + c^{36} + c^{33} + c^{21} + c^{18} + c^6 + c^3, \\
\end{align*}
\]

\[
a + d + c^{16} + c, \quad b + c^{16}, \\
d^3 + d^2 c + dc^2 + c^{192} + c^{144} + c^{132} + c^{129} + c^72 + c^48 + c^{33} + c^{24} + c^{18} + c^{12} + c^9 + 1, \\
d(c^{16} + c) + c^{176} + c^{161} + c^{146} + c^{131} + c^{80} + c^65 + c^56 + c^41 + c^26 + c^{20} + c^{17} + c^{11} + c^5 + c^2, \\
(c^{16} + c)(c^{192} + c^{144} + c^{132} + c^{129} + c^96 + c^72 + c^66 + c^48 + c^{36} + c^{33} + c^{24} + c^{18} + c^{12} + c^9 + c^6 + c^3 + 1). \\
\]

- The last element is a polynomial on \(c\) of degree 192. It is a product of 12 irreducible polynomials of degree 8 over \(\overline{\mathbb{F}_2}\). Total number of solutions in \(\overline{\mathbb{F}_2}\) is 480.
Example: $X_0(37)$ in characteristic 2

- Gröbner basis.

$$u_0 + u_3 + d^2c^4 + d^2c + dc^8 + dc^2 + c^{192} + c^{180} + c^{168} + c^{165} + c^{150} + c^{138} + c^{135} + c^{132} + c^{120} + c^{105} + c^{96} + c^{90} + c^{84} + c^{75} + c^{69} + c^{66} + c^{48} + c^{36} + c^{18} + c^{9},
\begin{align*}
u_1 &+ u_3 + d^2c + dc^8 + c^{168} + c^{138} + c^{120} + c^{105} + c^{90} + c^{75} + c^{72} + c^{60} + c^{48} + c^{45} + c^{30} + c^{24} + c^{18} + c^{15} + c^{12} + c^{3}, \\
u_2 &+ u_3 + d^2c^4 + dc^2 + c^{180} + c^{165} + c^{150} + c^{144} + c^{135} + c^{129} + c^{96} + c^{84} + c^{69} + c^{66} + c^{48} + c^{36} + c^{30} + c^{18} + c^{15}, \\
u_3 &+ u_3 + d^2c^4 + d^2c + dc^5 + dc^2 + c^{36} + c^{33} + c^{21} + c^{18} + c^{6} + c^{3}, \\
a &+ d + c^{16} + c, \\
b &+ c^{16}, \\
d^3 &+ d^2c + dc^2 + c^{192} + c^{144} + c^{132} + c^{129} + c^{72} + c^{48} + c^{33} + c^{24} + c^{18} + c^{12} + c^{9} + 1, \\
d &+ c^{16} + c, \\
d &+ c^{17} + c^{11} + c^5 + c^2, \\
\end{align*}$$

- The last element is a polynomial on $c$ of degree 192. It is a product of 12 irreducible polynomials of degree 8 over $\mathbb{F}_2$. Total number of solutions in $\overline{\mathbb{F}}_2$ is 480.
Example: \( X_0(37) \) in characteristic 2

However, since for each root \( \alpha \) 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

\[
|G| = 480/3 = 160, \quad |\bar{G}| = |G|/2 = 80.
\]

\( \bar{G} \) is the semi-direct product of an elementary abelian 2-group of order 16 by a cyclic group of order 5.

By using a restriction argument on \( H^2(\bar{G}, \mathbb{Z}/2\mathbb{Z}) \) we can see that the structure of the group in the middle is determined by the 2-Sylow subgroup which is isomorphic to the extraspecial group \( E_{32^-} \), which has 5 subgroups isomorphic to \( Q_8 \times (\mathbb{Z}/2\mathbb{Z}) \) and another 5 subgroup isomorphic to \( H_{16} \). The group \( G \) is a semi-direct product of \( E_{32^-} \) by a cyclic group of order 5.
Example: $X_0(37)$ in characteristic 2

- However, since for each root $\alpha$ 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

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

- $\overline{G}$ is the semi-direct product of an elementary abelian 2-group of order 16 by a cyclic group of order 5.

- By using a restriction argument on $H^2(\overline{G}, \mathbb{Z}/2\mathbb{Z})$ we can see that the structure of the group in the middle is determined by the 2-Sylow subgroup which is isomorphic to the extraspecial group $E_{32^-}$, which has 5 subgroups isomorphic to $Q_8 \times (\mathbb{Z}/2\mathbb{Z})$ and another 5 subgroup isomorphic to $H_{16}$. The group $G$ is a semi-direct product of $E_{32^-}$ by a cyclic group of order 5.
Example: $X_0(37)$ in characteristic 2

- However, since for each root $\alpha$ 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

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

- $\overline{G}$ is the semi-direct product of an elementary abelian 2-group of order 16 by a cyclic group of order 5.

- By using a restriction argument on $H^2(\overline{G}, \mathbb{Z}/2\mathbb{Z})$ we can see that the structure of the group in the middle is determined by the 2-Sylow subgroup which is isomorphic to the extraspecial group $E_{32-}$, which has 5 subgroups isomorphic to $Q_8 \times (\mathbb{Z}/2\mathbb{Z})$ and another 5 subgroup isomorphic to $H_{16}$. The group $G$ is a semi-direct product of $E_{32-}$ by a cyclic group of order 5.
### Automorphisms of Hyperelliptic Modular Curves

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>22</td>
<td>2</td>
<td>$(\mathbb{Z}/2\mathbb{Z})^2$</td>
<td>3, 29, 101</td>
<td>$D_6$, $D_4$</td>
</tr>
<tr>
<td>23</td>
<td>2</td>
<td>$\mathbb{Z}/2\mathbb{Z}$</td>
<td>3, 13, 29, 43, 101, 5623</td>
<td>$D_2$</td>
</tr>
<tr>
<td>26</td>
<td>2</td>
<td>$(\mathbb{Z}/2\mathbb{Z})^2$</td>
<td>7, 31, 41, 89</td>
<td>$D_6$, $D_4$</td>
</tr>
<tr>
<td>28</td>
<td>2</td>
<td>$D_6$</td>
<td>3, 5, 11</td>
<td>$GL_2(3)$, $B$, $V_6$</td>
</tr>
<tr>
<td>29</td>
<td>2</td>
<td>$\mathbb{Z}/2\mathbb{Z}$</td>
<td>19, 5, 67, 137, 51241</td>
<td>$D_4$, $D_2$</td>
</tr>
<tr>
<td>30</td>
<td>3</td>
<td>$(\mathbb{Z}/2\mathbb{Z})^3$</td>
<td>23</td>
<td>$V_8$</td>
</tr>
</tbody>
</table>

On the Automorphism Groups of modular curves $X_0(N)$
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>31</td>
<td>2</td>
<td>$\mathbb{Z}/2\mathbb{Z}$</td>
<td>3, 5, 11, 37, 67, 131, 149</td>
<td>$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$, $D_2$</td>
</tr>
<tr>
<td>33</td>
<td>3</td>
<td>$(\mathbb{Z}/2\mathbb{Z})^3$</td>
<td>2, 19, 47</td>
<td>$\text{GL}_2(2) \times \mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$, $(\mathbb{Z}/2\mathbb{Z})^3$</td>
</tr>
<tr>
<td>35</td>
<td>3</td>
<td>$(\mathbb{Z}/2\mathbb{Z})^2$</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>37</td>
<td>2</td>
<td>$(\mathbb{Z}/2\mathbb{Z})^2$</td>
<td>2, 3, 7, 31, 29, 61</td>
<td>$E_{32-} \rtimes (\mathbb{Z}/5\mathbb{Z})$, $\mathbb{Z}/3\mathbb{Z} \times (\mathbb{Z}/2\mathbb{Z})^2$, $D_6$, $D_4$</td>
</tr>
<tr>
<td>39</td>
<td>3</td>
<td>$(\mathbb{Z}/2\mathbb{Z})^2$</td>
<td>5</td>
<td>$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$, $(\mathbb{Z}/2\mathbb{Z})^2$</td>
</tr>
</tbody>
</table>
## Automorphisms of Hyperelliptic Modular Curves

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>41</td>
<td>3</td>
<td>$\mathbb{Z}/2\mathbb{Z}$</td>
<td>17</td>
<td>$D_2$</td>
</tr>
<tr>
<td>46</td>
<td>5</td>
<td>$(\mathbb{Z}/2\mathbb{Z})^2$</td>
<td>3</td>
<td>$(\mathbb{Z}/2\mathbb{Z})^3$</td>
</tr>
<tr>
<td>47</td>
<td>4</td>
<td>$\mathbb{Z}/2\mathbb{Z}$</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>48</td>
<td>3</td>
<td>$\mathbb{Z}/2\mathbb{Z} \times S_4$</td>
<td>7</td>
<td>$A,</td>
</tr>
<tr>
<td>50</td>
<td>2</td>
<td>$(\mathbb{Z}/2\mathbb{Z})^2$</td>
<td>3, 37</td>
<td>$D_6, D_4$</td>
</tr>
<tr>
<td>59</td>
<td>5</td>
<td>$\mathbb{Z}/2\mathbb{Z}$</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>71</td>
<td>6</td>
<td>$\mathbb{Z}/2\mathbb{Z}$</td>
<td>—</td>
<td>—</td>
</tr>
</tbody>
</table>
The canonical embedding

**Theorem**

Let $\omega_1, \ldots, \omega_g$ be a basis of $H^0(X_0(N), \Omega^1)$, and suppose that $X_0(N)$ is not hyperelliptic. The map

$$
\Phi : X_0(N) \to \mathbb{P}^{g-1},
$$

$$
P \mapsto (1 : \frac{\omega_2}{\omega_1} : \ldots : \frac{\omega_g}{\omega_1})
$$

gives an embedding of $X_0(N)$ in $\mathbb{P}^{g-1}$.

Every automorphism of $X_0(N)$ is the restriction of an automorphism of the ambient space $\mathbb{P}^{g-1}$.

The automorphism group of $\mathbb{P}^{g-1}_k$ equals $\text{PGL}(g, k)$. 

On the Automorphism Groups of modular curves $X_0(N)$
**$g = 3$, non hyperelliptic**

- All non-hyperelliptic curves of genus 3 are hypersurfaces in $\mathbb{P}^2$.

<table>
<thead>
<tr>
<th>$X_0(N)$</th>
<th>Equation</th>
</tr>
</thead>
<tbody>
<tr>
<td>$X_0(34)$</td>
<td>$x^4 + y^4 - z^4 + x^3y + xy^3 - 2x^2y^2 + 3xyz^2 = 0$</td>
</tr>
<tr>
<td>$X_0(43)$</td>
<td>$2x^3y + 6x^2y^2 + 11xy^3 + 9y^4 - x^3z - 6x^2yz - 14xy^2z - 12y^3z + 2x^2z^2 + 8xyz^2 + 10y^2z^2 - xz^3 + z^4 = 0$</td>
</tr>
<tr>
<td>$X_0(45)$</td>
<td>$x^4 + y^4 + 81z^4 - 2x^2y^2 - 2x^2y^2 - 2x^2z^2 - 18y^2z^2 - 16xy^2z = 0$</td>
</tr>
<tr>
<td>$X_0(64)$</td>
<td>$x^4 + y^4 - z^4 = 0$</td>
</tr>
</tbody>
</table>
\( g = 3, \text{ non hyperelliptic} \)

All non-hyperelliptic curves of genus 3 are hypersurfaces in \( \mathbb{P}^2 \).

<table>
<thead>
<tr>
<th>( X_0(N) )</th>
<th>Equation</th>
</tr>
</thead>
<tbody>
<tr>
<td>( X_0(34) )</td>
<td>( x^4 + y^4 - z^4 + x^3y + xy^3 - 2x^2y^2 + 3xyz^2 = 0 )</td>
</tr>
<tr>
<td>( X_0(43) )</td>
<td>( 2x^3y + 6x^2y^2 + 11xy^3 + 9y^4 - x^3z - 6x^2yz - 14xy^2z - 12y^3z + 2x^2z^2 + 8xyz^2 + 10y^2z^2 - xz^3 + z^4 = 0 )</td>
</tr>
<tr>
<td>( X_0(45) )</td>
<td>( x^4 + y^4 + 81z^4 - 2x^2y^2 - 2x^2y^2 - 2x^2z^2 - 18y^2z^2 - 16xy^2z = 0 )</td>
</tr>
<tr>
<td>( X_0(64) )</td>
<td>( x^4 + y^4 - z^4 = 0 )</td>
</tr>
</tbody>
</table>
Linear automorphisms

- **Idea:** Compute all matrices $A = (a_{ij})$ such that

$$f(Ax) = \lambda_A f(x).$$

- Difficult problem to solve.
Linear automorphisms

- **Idea:** Compute all matrices $A = (a_{ij})$ such that

  $$f(Ax) = \lambda_A f(x).$$

- Difficult problem to solve.
Projective Duality

- Consider the Gauss map

\[ X \rightarrow X^* \]

\[ (x_0, x_1, x_2) \mapsto \left( \frac{\partial f}{\partial x} : \frac{\partial f}{\partial y} : \frac{\partial f}{\partial z} \right) \bigg|_{(x_0, y_0, z_0)} \]

- Every automorphism induces a linear action (by $A^{-1}$) on the dual curve.

- A simpler problem (the derivatives are simpler than the original polynomials)
Consider the Gauss map

$$X \rightarrow X^*$$

$$(x_0, x_1, x_2) \mapsto \left( \frac{\partial f}{\partial x} : \frac{\partial f}{\partial y} : \frac{\partial f}{\partial z} \right) \bigg|_{(x_0, y_0, z_0)}$$

Every automorphism induces a linear action (by $A^{-1}$) on the dual curve.

A simpler problem (the derivatives are simpler than the original polynomials)
Consider the Gauss map

\[ X \rightarrow X^* \]

\[ (x_0, x_1, x_2) \mapsto \left( \frac{\partial f}{\partial x} : \frac{\partial f}{\partial y} : \frac{\partial f}{\partial z} \right) \bigg|_{(x_0, y_0, z_0)} \]

Every automorphism induces a linear action (by $A^{-1}$) on the dual curve.

A simpler problem (the derivatives are simpler than the original polynomials)
Example: $X_0(64)$

\[ Y_1 := \frac{\partial f}{\partial x} = 4x^3, \quad Y_2 := \frac{\partial f}{\partial y} = 4y^3, \quad Y_3 := \frac{\partial f}{\partial z} = -4z^3 \]

Find $a_{ij}$ such that

\[ 4 \left( \sum_{\nu=1}^{3} a_{i\nu} x_{\nu} \right)^3 = b_{11} Y_1 + b_{12} Y_2 + b_{13} Y_3 \text{ etc} \]

The group is bigger than $(\mu_4 \times \mu_4) \rtimes S_3$ only in characteristic $3$, since then raising to the third power is linear!

$\text{Aut}(X_0(64), 3) \cong \text{PGU}(3, \mathbb{F}_9)$. 

On the Automorphism Groups of modular curves $X_0(N)$
Example: $X_0(64)$

- $Y_1 := \frac{\partial f}{\partial x} = 4x^3$, $Y_2 := \frac{\partial f}{\partial y} = 4y^3$, $Y_3 := \frac{\partial f}{\partial z} = -4z^3$

- Find $a_{ij}$ such that

$$4 \left( \sum_{\nu=1}^{3} a_{\nu} x_{\nu} \right)^3 = b_{11} Y_1 + b_{12} Y_2 + b_{13} Y_3 \text{ etc}$$

The group is bigger than $(\mu_4 \times \mu_4) \rtimes S_3$ only in characteristic 3, since then raising to the third power is linear!

- $\text{Aut}(X_0(64), 3) \cong \text{PGU}(3, \mathbb{F}_9)$. 
Example: $X_0(64)$

\[ Y_1 := \frac{\partial f}{\partial x} = 4x^3, \quad Y_2 := \frac{\partial f}{\partial y} = 4y^3, \quad Y_3 := \frac{\partial f}{\partial z} = -4z^3 \]

Find $a_{ij}$ such that

\[ 4 \left( \sum_{\nu=1}^{3} a_{i\nu} x_{\nu} \right)^3 = b_{11} Y_1 + b_{12} Y_2 + b_{13} Y_3 \text{etc} \]

The group is bigger than $(\mu_4 \times \mu_4) \rtimes S_3$ only in characteristic 3, since then raising to the third power is linear!

\[ \text{Aut}(X_0(64), 3) \cong \text{PGU}(3, \mathbb{F}_9). \]