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

Motivation

Let $\mathcal{X} \to S$ be a family of curves over a base scheme S.

For every point $P : \mathrm{Spec} k \to S$, we will consider the *absolute* automorphism group of the fiber P to be the automorphism group $\mathrm{Aut}_{\bar{k}}(\mathcal{X} \times_S \mathrm{Spec}\bar{k})$ 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 $P : \mathrm{Spec} k \to S$, we will consider the *absolute* automorphism group of the fiber P to be the automorphism group $\mathrm{Aut}_{\bar{k}}(\mathcal{X} \times_S \mathrm{Spec} \bar{k})$ 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 $P : \mathrm{Spec} k \to S$, we will consider the *absolute* automorphism group of the fiber P to be the automorphism group $\mathrm{Aut}_{\bar{k}}(\mathcal{X} \times_S \mathrm{Spec} \bar{k})$ 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 $\mathbb{Q}, \bar{\mathbb{Q}}, \mathbb{R}, \mathbb{C}, \mathbb{F}_p, \bar{\mathbb{F}}_p$ 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 $\mathbb{Q}, \bar{\mathbb{Q}}, \mathbb{R}, \mathbb{C}, \mathbb{F}_p, \bar{\mathbb{F}}_p$ etc.

Fermat Curves

- The Fermat Equation

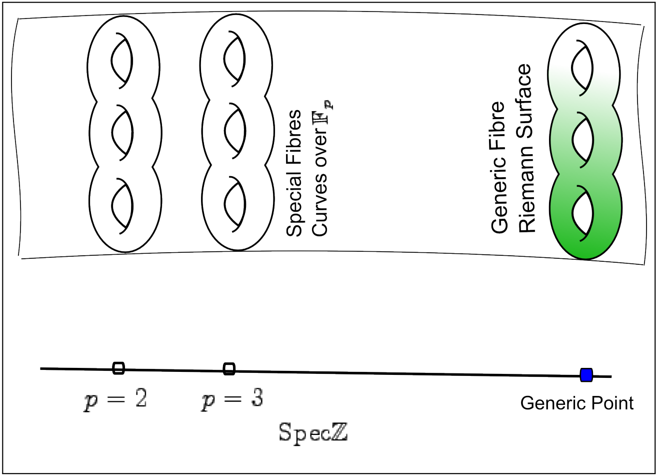
$$x^{p^s+1} + y^{p^s+1} + z^{p^s+1}$$

- 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 $\mathbb{Q}, \bar{\mathbb{Q}}, \mathbb{R}, \mathbb{C}, \mathbb{F}_p, \bar{\mathbb{F}}_p$ etc.

Arithmetic Surfaces



Stable Curves

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

$$\mathrm{Aut}(\mathcal{X}_\eta) \subseteq \mathrm{Aut}(\mathcal{X}_P)$$

Fermat Curves

- 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 $\mathrm{Spec}\mathbb{Z}[\frac{1}{p^s+1}]$

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

Tzermias, Leopoldt, Shioda.

Exceptional Fibers

- A special fibre $\mathcal{X}_p := \mathcal{X} \times_S S/p$ with $\mathrm{Aut}(\mathcal{X}_p) > \mathrm{Aut}(\mathcal{X}_\eta)$ 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.

Modular Curves

- $\Gamma = \mathrm{PSL}(2, \mathbb{Z})$
- $\Gamma(N) := \{\sigma \in \Gamma : \sigma \equiv \mathbb{I}_2 \bmod N\}$
- $\Gamma_0(N) := \left\{\sigma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma : c \equiv 0 \bmod N\right\}$
- $Y(N) := \mathbb{H}/\Gamma(N)$, $Y_0(N) = \mathbb{H}/\Gamma_0(N)$
- $X(N) = Y(N) \cup \text{cusps}$, $X_0(N) = Y_0(N) \cup \text{cusps}$

Modular Curves

- $\Gamma = \mathrm{PSL}(2, \mathbb{Z})$
- $\Gamma(N) := \{\sigma \in \Gamma : \sigma \equiv \mathbb{I}_2 \bmod N\}$
- $\Gamma_0(N) := \left\{\sigma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma : c \equiv 0 \bmod N\right\}$
- $Y(N) := \mathbb{H}/\Gamma(N)$, $Y_0(N) = \mathbb{H}/\Gamma_0(N)$
- $X(N) = Y(N) \cup \text{cusps}$, $X_0(N) = Y_0(N) \cup \text{cusps}$

Modular Curves

- $\Gamma = \mathrm{PSL}(2, \mathbb{Z})$
- $\Gamma(N) := \{\sigma \in \Gamma : \sigma \equiv \mathbb{I}_2 \bmod N\}$
- $\Gamma_0(N) := \left\{ \sigma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma : c \equiv 0 \bmod N \right\}$
- $Y(N) := \mathbb{H}/\Gamma(N)$, $Y_0(N) = \mathbb{H}/\Gamma_0(N)$
- $X(N) = Y(N) \cup \text{cusps}$, $X_0(N) = Y_0(N) \cup \text{cusps}$

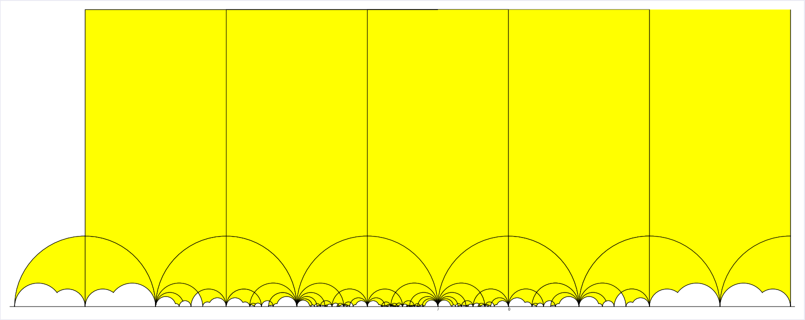
Modular Curves

- $\Gamma = \mathrm{PSL}(2, \mathbb{Z})$
- $\Gamma(N) := \{\sigma \in \Gamma : \sigma \equiv \mathbb{I}_2 \bmod N\}$
- $\Gamma_0(N) := \left\{\sigma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma : c \equiv 0 \bmod N\right\}$
- $Y(N) := \mathbb{H}/\Gamma(N),\ Y_0(N) = \mathbb{H}/\Gamma_0(N)$
- $X(N) = Y(N) \cup \text{cusps},\ X_0(N) = Y_0(N) \cup \text{cusps}$

Modular Curves

- $\Gamma = \mathrm{PSL}(2, \mathbb{Z})$
- $\Gamma(N) := \{\sigma \in \Gamma : \sigma \equiv \mathbb{I}_2 \bmod N\}$
- $\Gamma_0(N) := \left\{\sigma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma : c \equiv 0 \bmod N\right\}$
- $Y(N) := \mathbb{H}/\Gamma(N)$, $Y_0(N) = \mathbb{H}/\Gamma_0(N)$
- $X(N) = Y(N) \cup \text{cusps}$, $X_0(N) = Y_0(N) \cup \text{cusps}$

Fundamental Domain for $X_0(30)$



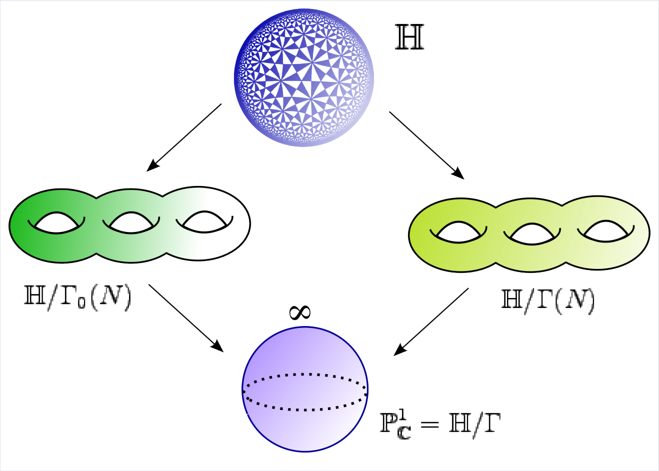
Automorphisms of Modular Curves over $\mathbb{C}$

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

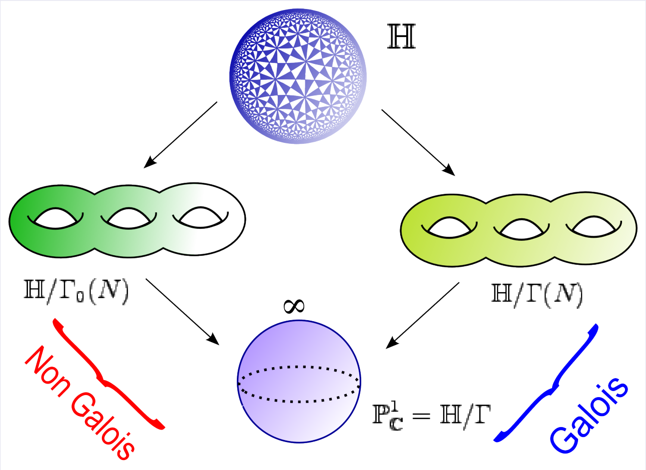
Automorphisms of Modular Curves over $\mathbb{C}$

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

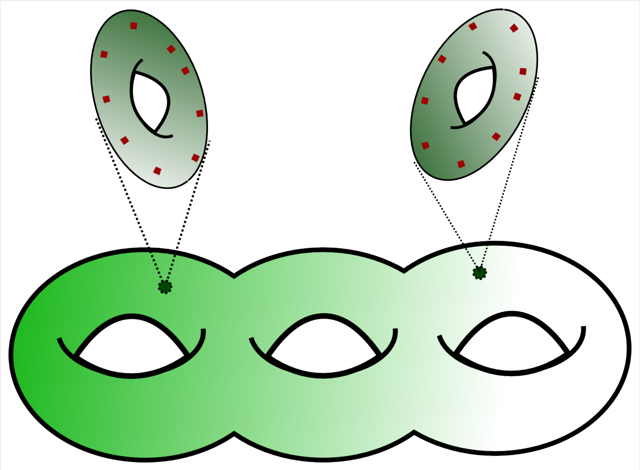
Modular Curves



Modular Curves



Moduli Interpretation



Modular Curves over Families

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 $\mathcal{X}_0(N) \rightarrow \mathbb{Z}[1/N]$ so that for $p \in \mathrm{Spec}\mathbb{Z}[1/N]$ the reduction $\mathcal{X}_0(N) \times_{\mathrm{Spec}\mathbb{Z}} \mathbb{F}_p$ is the moduli space of elliptic curves with a fixed cyclic subgroup of order N.

Variation of automnorphisms: $X(N)$ case

- A. Adler in 97 and C.S. Rajan in 98 proved for $X(N)$, that $X(11)_3 := X(11) \times_{\mathrm{Spec}\mathbb{Z}} \mathrm{Spec}\mathbb{F}_3$ has the Mathiew 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 varius primes p. It turns out that the reduction $X(7)_3$ of $X(7)$ at the prime p has automorphism group $\mathrm{PGU}(3,3)$ and these are the only cases where $\mathrm{Aut}X(q)_p > \mathrm{Aut}X(q) \cong \mathrm{PSL}(2,p)$.

Variation of automnorphisms: $X(N)$ case

- A. Adler in 97 and C.S. Rajan in 98 proved for $X(N)$, that $X(11)_3 := X(11) \times_{\mathrm{Spec}\mathbb{Z}} \mathrm{Spec}\mathbb{F}_3$ has the Mathiew 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 varius primes p. It turns out that the reduction $X(7)_3$ of $X(7)$ at the prime p has automorphism group $\mathrm{PGU}(3,3)$ and these are the only cases where $\mathrm{Aut}X(q)_p > \mathrm{Aut}X(q) \cong \mathrm{PSL}(2,p)$.

Hyperelliptic modular curves

22	$y^2 = (x^3+4x^2+8x+4)(x^3+8x^2+16x+16)$
23	$y^2 = (x^3-x+1)(x^3-8x^2+3x-7)$
26	$y^2 = x^6-8x^5+8x^4-18x^3+8x^2-8x+1$
28	$y^2 = (x^2+7)(x^2+x+2)(x^2-x+2)$
29	$y^2 = x^6-4x^5-12x^4+2x^3+8x^2+8x-7$
30	$y^2 = (x^2+4x-1)(x^2+x-1)(x^4+x^3+2x^2-x+1)$
31	$y^2 = (x^3-6x^2-5x-1)(x^3-2x^2-x+3)$
33	$y^2 = (x^2+x+3)(x^6+7x^5+28x^4+59x^3+84x^2+63x+27)$
35	$y^2 = (x^2+x-1)(x^6-5x^5-9x^3-5x-1)$
37	$y^2 = x^6+14x^5+35x^4+48x^3+35x^2+14x+1$
39	$y^2 = (x^4-7x^3+11x^2-7x+1)(x^4+x^3-x^2+x+1)$
40	$y^2 = x^8+8x^6-2x^4+8x^2+1$
41	$y^2 = x^8-4x^7-8x^6+10x^5+20x^4+8x^3-15x^2-20x-8$
46	$y^2 = (x^3+x^2+2x+1)(x^3+4x^2+4x+8)(x^6+5x^5+14x^4+25x^3+28x^2+20x+8)$
47	$y^2 = (x^5+4x^4+7x^3+8x^2+4x+1)(x^5-5x^3-20x^2-24x-19)$
48	$y^2 = (x^4-2x^3+2x^2+2x+1)(x^4+2x^3+2x^2-2x+1) = x^8+14x^4+1$
50	$y^2 = x^6-4x^5-10x^3-4x+1$
59	$y^2 = (x^3+2x^2+1)(x^9+2x^8-4x^7-21x^6-44x^5-60x^4-61x^3-46x^2-24x-11)$
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.

Hyperelliptic modular curves

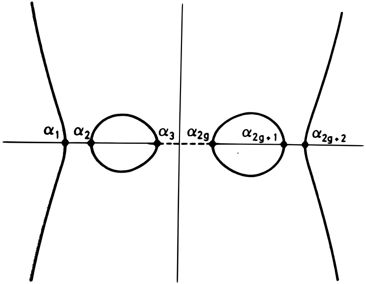
- The above list is due to M. Shimura (1995) and Galbraith (1996)
- The above models are not the Igusa models. They are singular at infinity and singular at the fibers over the prime 2.
- For the prime 2 we will seek another model (Artin-Schreier extension).
- For all fibers above $p \neq 2$ we can work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

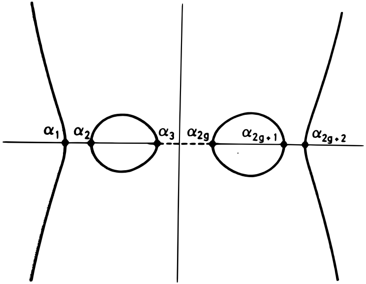
Real Points Hyperelliptic curves

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



Real Points Hyperelliptic curves

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

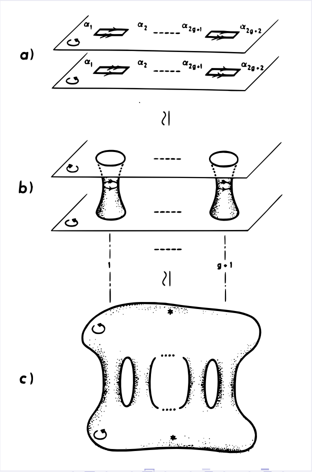


Complex Points Hyperelliptic curves

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

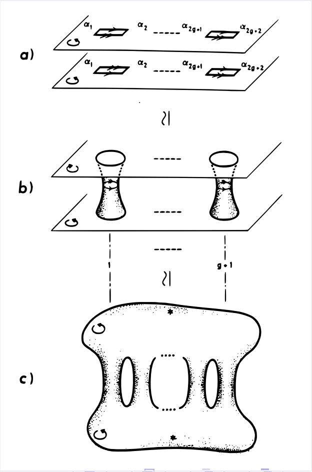


Complex Points Hyperelliptic curves

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

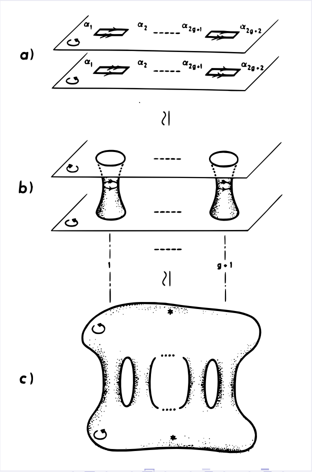


Complex Points Hyperelliptic curves

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

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

The structure of the group $\mathrm{Aut}(C)$ 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 α_i.

Automorphisms of Hyperelliptic curves $p \neq 2$

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

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

The structure of the group $\mathrm{Aut}(C)$ 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 α_i.

Automorphisms of Hyperelliptic curves $p \neq 2$

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

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

The structure of the group $\mathrm{Aut}(C)$ 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 α_i.

Automorphisms of Hyperelliptic curves $p \neq 2$

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

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

The structure of the group $\mathrm{Aut}(C)$ 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 α_i.

Automorphisms of Hyperelliptic curves $p \neq 2$

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

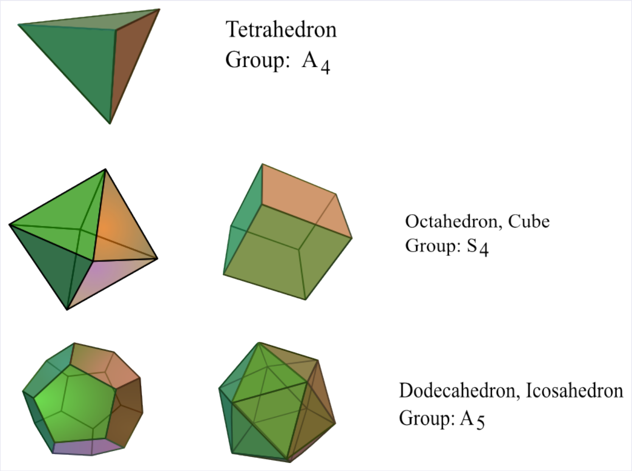
$$1 \to \langle j \rangle \to \mathrm{Aut}(C) \to H \to 1.$$

The structure of the group $\mathrm{Aut}(C)$ 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 α_i.

Finite subgroups of $\mathrm{PGL}(2, k)$

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

Platonic Solids



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 $\sigma' : x \mapsto \zeta_6 x$.

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 $\sigma' : x \mapsto \zeta_6 x$.

Hyperelliptic Curves with an extra involution

- 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.

Hyperelliptic Curves with an extra involution

- 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 $u_i := a_1^{g-i+1} a_i + a_g^{g-i+1} a_{g-i+1}$ 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 $i = 1, \ldots, g$

$g = 2$

Theorem

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.
   1. $\mathrm{GL}_2(3)$ *if and only if* $(u_1, u_2) = (-250, 50)$ *and* $p \neq 5$
   2. 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* $2u_1^2 - u_2^3$ *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:*

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

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

$g = 3$

- A similar theorem holds. Too complicated to write it down!
- An additional difficulty: The *normalized* models are defined over a PID different than $\mathbb{Z}$.

N	$f(x)$
30	$x^8 + \frac{\left(276+184\sqrt{2}\right)}{\left(-540\sqrt{2}-765\right)} x^6 - 46\, x^4 + \frac{\left(-184\sqrt{2}+276\right)}{\left(-540\sqrt{2}-765\right)} x^2 - \frac{765+540\sqrt{2}}{\left(-540\sqrt{2}-765\right)}$
33	$x^8 + \frac{\left(-240\sqrt{3}+508\right)x^6}{-264\sqrt{3}+473} + 342\, x^4 + \frac{\left(508+240\sqrt{3}\right)x^2}{-264\sqrt{3}+473} + \frac{473+264\sqrt{3}}{-264\sqrt{3}+473}$
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	$x^8 + 14x^4 + 1$

$g = 3$

- A similar theorem holds. Too complicated to write it down!
- An additional difficulty: The *normalized* models are defined over a PID different than $\mathbb{Z}$.

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

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 $\mathrm{PGL}(2,7)$ by $\mathbb{Z}/2\mathbb{Z}$. Using magma we compute that this group admits the following presentation:

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

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 $\mathrm{PGL}(2,7)$ by $\mathbb{Z}/2\mathbb{Z}$. Using magma we compute that this group admits the following presentation:

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

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 $\mathrm{PGL}(2,7)$ by $\mathbb{Z}/2\mathbb{Z}$. Using magma we compute that this group admits the following presentation:

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

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 σ 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 σ 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 σ 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 σ 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 σ 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 σ 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 σ 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 σ 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.

Gröbner Bases

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

Gröbner Bases

- Consider the ideal $I_r := \langle a_i, i = 1, \dots, r \rangle \lhd \mathbb{Z}[a, b, c, d]$ 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^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.
- Consider the same system modulo $\bar{\mathbb{F}}_p$

Gröbner Bases

- Consider the ideal $I_r := \langle a_i, i = 1, \dots, r \rangle \lhd \mathbb{Z}[a, b, c, d]$ 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^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.
- Consider the same system modulo $\bar{\mathbb{F}}_p$

Gröbner Bases

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

Example: $N = 41$

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

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 $\bar{\mathbb{F}}_{17}$. 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 σ so that $\bar{\sigma} : x \mapsto \frac{-9bx+b}{-8bx-9b} = \frac{9x-1}{8x+9}$. The automorphism group in this case is $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

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 $\bar{\mathbb{F}}_{17}$. 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 σ so that $\bar{\sigma} : x \mapsto \frac{-9bx+b}{-8bx-9b} = \frac{9x-1}{8x+9}$. The automorphism group in this case is $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

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 $\bar{\mathbb{F}}_{17}$. 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 σ 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 $\deg q(x) \le g + 1$ and $\deg p(x) \le 2g + 1$. (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 $(x, Y) \mapsto (x, Y + 1)$.

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 $(x, Y) \mapsto (x, Y+1)$.

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 $(x, Y) \mapsto (x, Y+1)$.

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 $(x, Y) \mapsto (x, Y + 1)$.

Automorphisms of Weierstrass Models

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

Automorphisms of Weierstrass Models

- A basis for the space of holomorphic differentials on C is given by
$$\omega_i = \frac{x^{i-1}dx}{2y+q} = \frac{x^{i-1}dx}{q}, \quad 1 \le i \le g,$$
- Every automorphism σ of C induces a linear action on the space of holomorphic differentials.
- Write $q((ax+b)/(cx+d))(cx+d)^{g+1} = q^*(x) \in \overline{\mathbb{F}}_2[x]$.
- $q^* = \lambda q$

Automorphisms of Weierstrass Models

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

Automorphisms of Weierstrass Models

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

Automorphisms of Weierstrass Models

Theorem

Let $C := y^2 + q(x)y + p(x)$ *be a hyperelliptic curve of genus* g *over* $\bar{\mathbb{F}}_2$ *with* $\deg q(x) \leq g+1$ *and* $\deg p(x) \leq 2g+1$. *Then every automorphism* σ *of* 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 $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}_2(\bar{\mathbb{F}}_2)$ *and* $h(x) \in \bar{\mathbb{F}}_2[x]$ *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.

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

- 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 $\bar{\mathbb{F}}_2$ is 480.

Example: $X_0(37)$ in characteristic 2

- Gröbner basis.

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

- 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 $\bar{\mathbb{F}}_2$ is 480.

Example: $X_0(37)$ in characteristic 2

- 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

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

- $\overline{G}$ 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 $H^2(\bar{G},\mathbb{Z}/2\mathbb{Z})$ we can see that the structure of the group in the midle is determined by the 2-Syllow 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 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

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

- $\overline{G}$ 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 $H^2(\bar{G}, \mathbb{Z}/2\mathbb{Z})$ we can see that the structure of the group in the midle is determined by the 2-Syllow 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 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

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

- $\overline{G}$ 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 $H^2(\bar{G}, \mathbb{Z}/2\mathbb{Z})$ we can see that the structure of the group in the midle is determined by the 2-Syllow 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

N	Genus	Generic Aut.	Exceptional primes	Except. Aut.
22	2	$(\mathbb{Z}/2\mathbb{Z})^2$	$3, 29$	D_6
			101	D_4
23	2	$\mathbb{Z}/2\mathbb{Z}$	$3, 13, 29, 43, 101, 5623$	D_2
26	2	$(\mathbb{Z}/2\mathbb{Z})^2$	$7, 31$	D_6
			$41, 89$	D_4
28	2	D_6	3	$\mathrm{GL}_2(3)$
			5	B
			11	V_6
29	2	$\mathbb{Z}/2\mathbb{Z}$	19	D_4
			$5, 67, 137, 51241$	D_2
30	3	$(\mathbb{Z}/2\mathbb{Z})^3$	23	V_8

Automorphisms of Hyperelliptic Modular Curves

-

N	Genus	Generic Aut	Exceptional primes	Except. Aut.
31	2	$\mathbb{Z}/2\mathbb{Z}$	3	$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$
			5,	D_2
			$11, 37, 67, 131, 149$	
33	3	$(\mathbb{Z}/2\mathbb{Z})^3$	2	$\mathrm{GL}_2(2) \times \mathbb{Z}/2\mathbb{Z}$
			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	$E_{32-} \rtimes (\mathbb{Z}/5\mathbb{Z})$
			3	$\mathbb{Z}/3\mathbb{Z} \times (\mathbb{Z}/2\mathbb{Z})$
			$7, 31$	D_6
			$29, 61$	D_4
39	3	$(\mathbb{Z}/2\mathbb{Z})^2$	5	$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$

Automorphisms of Hyperelliptic Modular Curves

N	Genus	Generic Aut	Exceptional primes	Except. Aut.
41	3	$\mathbb{Z}/2\mathbb{Z}$	17	D_2
46	5	$(\mathbb{Z}/2\mathbb{Z})^2$	3	$(\mathbb{Z}/2\mathbb{Z})^3$
47	4	$\mathbb{Z}/2\mathbb{Z}$	—	—
48	3	$\mathbb{Z}/2\mathbb{Z} \times S_4$	7	A, $\lvert A\rvert = 672$
50	2	$(\mathbb{Z}/2\mathbb{Z})^2$	3	D_6
			37	D_4
59	5	$\mathbb{Z}/2\mathbb{Z}$	—	—
71	6	$\mathbb{Z}/2\mathbb{Z}$	—	—

The canonical embedding

Theorem

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

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

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

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 $\mathbb{P}_k^{g-1}$ equals $\mathrm{PGL}(g, k)$.

$g = 3$, non hyperelliptic

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

$X_0(34)$	$x^4 + y^4 - z^4 + x^3y + xy^3 - 2x^2y^2 + 3xyz^2 = 0$
$X_0(43)$	$2x^3y + 6x^2y^2 + 11xy^3 + 9y^4 - x^3z - 6x^2yz - 14xy^2z$ $-12y^3z + 2x^2z^2 + 8xyz^2 + 10y^2z^2 - xz^3 + z^4 = 0$
$X_0(45)$	$x^4 + y^4 + 81z^4 - 2x^2y^2 - 2x^2y^2 - 2x^2z^2 -$ $18y^2z^2 - 16xy^2z = 0$
$X_0(64)$	$x^4 + y^4 - z^4 = 0$

$g = 3$, non hyperelliptic

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

$X_0(34)$	$x^4 + y^4 - z^4 + x^3y + xy^3 - 2x^2y^2 + 3xyz^2 = 0$
$X_0(43)$	$2x^3y + 6x^2y^2 + 11xy^3 + 9y^4 - x^3z - 6x^2yz - 14xy^2z$ $-12y^3z + 2x^2z^2 + 8xyz^2 + 10y^2z^2 - xz^3 + z^4 = 0$
$X_0(45)$	$x^4 + y^4 + 81z^4 - 2x^2y^2 - 2x^2y^2 - 2x^2z^2 -$ $18y^2z^2 - 16xy^2z = 0$
$X_0(64)$	$x^4 + y^4 - z^4 = 0$

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

$$X \to X^*$$

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

- Every automorphism induces a linear action (by A^{-1}) on the dual curve.
- A simpler problem (the derivatives are simpler than the original polynomials)

Projective Duality

- Consider the Gauss map

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

- Every automorphism induces a linear action (by A^{-1}) on the dual curve.
- A simpler problem (the derivatives are simpler than the original polynomials)

Projective Duality

- Consider the Gauss map

$$X \to X^*$$

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

- 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: $X_0(64)$

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

- Find a_{ij} such that

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

  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!

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

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

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

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
$$4\left(\sum_{\nu=1}^{3} a_{i\nu}x_\nu\right)^3 = b_{11}Y_1 + b_{12}Y_2 + b_{13}Y_3\text{etc}$$
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!
- $\mathrm{Aut}(X_0(64), 3) \cong \mathrm{PGU}(3, \mathbb{F}_9)$.