Automorphisms of Modular Curves $X(n)$

Barcelona March 2004.

$$1 \longrightarrow \Gamma(N) \longrightarrow PSL(2,\mathbb{Z}) \longrightarrow PSL(2,\mathbb{Z}/N\mathbb{Z}) \longrightarrow 1$$

$$\Gamma(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in PSL(2,\mathbb{Z}) : \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \bmod N \right\}$$

$$\Gamma(N) \backslash \mathbb{H} = Y(N) \longrightarrow X(N)$$

$$PSL(2,\mathbb{Z}/N\mathbb{Z}) = \frac{N_{PSL(2,\mathbb{Z})}\,\Gamma(N)}{\Gamma(N)} \subseteq \operatorname{Aut} X(N)$$

J. P. Serre: Appendix on a paper of Mazur

$N = p$ is a prime number.

$$\begin{array}{c} X(N) \\ \Big\downarrow {\scriptstyle PSL(2,\mathbb{Z}/N\mathbb{Z})} \\ \mathbb{P}^1(\mathbb{C}) \end{array} \qquad \begin{array}{c} 2 \Big| \\ \cdot \\ j(i) \end{array} \qquad \begin{array}{c} 3 \Big| \\ \cdot \\ j(\omega) \end{array} \qquad \begin{array}{c} \Big| N \\ \cdot \\ j(\infty) \end{array}$$

$$PSL(2,\tfrac{\mathbb{Z}}{N\mathbb{Z}}) =: \mu_N = \begin{cases} \dfrac{N^3}{2} \prod_{p \mid N} \left(1 - \frac{1}{p^2}\right) & N > 2 \\ 6 & N = 2 \end{cases}$$

$$g_N = 1 + \mu_N \frac{N-6}{12N}.$$

If $PSL(2, \mathbb{Z}/N\mathbb{Z}) \triangleleft Aut(X(N))$

Every automorphism of $Aut\, X(N)$ is restricted to automorphism of $\mathbb{P}^1$ fixing 3 points $\Rightarrow \sigma$ is the identity. $\Rightarrow Aut(X(N)) = PSL(2, \mathbb{Z}/N\mathbb{Z})$

$$m := [Aut(X(N) : Gal(X(N)/X(1))]$$

$N \neq 2$

$84(g_N - 1) = |PSL(2, \mathbb{Z}/N\mathbb{Z})| \left(7 - \frac{42}{N}\right).$

Hurwitz Bound: $char\, k = 0 \Rightarrow |Aut\, X(N)| \leq 84(g_N - 1)$

$m \leq 2$	$7 \leq N < 11$	$\Rightarrow Aut\, X(N) \cong PSL(2, \mathbb{Z}/N\mathbb{Z})$
$m \leq 3$	$11 \leq N \leq 14$	
$m \leq 4$	$14 \leq N < 21$	
$m < 7$	$21 \leq N$	

We will prove that $PSL(2, \mathbb{Z}/N\mathbb{Z}) \triangleleft Aut\, X(N)$.

$$\theta : PSL(2, \mathbb{Z}/N\mathbb{Z}) \longmapsto S_m$$
$$\sigma \longmapsto \{\sigma\alpha_1 PSL(2, \mathbb{Z}/N\mathbb{Z}), \sigma\alpha_2 PSL(2, \mathbb{Z}/N\mathbb{Z}), \ldots, \sigma\alpha_m PSL\}$$

$\{\alpha_1 PSL(2, \mathbb{Z}/N\mathbb{Z}), \ldots, \alpha_m PSL(2, \mathbb{Z}/N\mathbb{Z})\}$ cosets of $Aut\, X(N)$

Case 1 $N = p \geq 7$

$PSL(2, p)$ simple $\Rightarrow \ker\theta = PSL(2, p)$ or $\{1\}$

If $\ker\theta = \{1\}$ then

$PSL(2, p) < S_m$ imposible: there are no ellements of order p in S_m, $\underline{\underline{m \leq 6}}$

$$\begin{tikzcd} X(p^e) \arrow[d] \\ X(p) \arrow[d] \\ X(1) \end{tikzcd} \qquad \begin{array}{l} H = Gal(X(p^e)/X(p)) \\ \\ PSL(2,p) \end{array}$$

$PSL(2, \mathbb{Z}/p^e\mathbb{Z})$

$$H = p^{3(e-1)}, \quad p \geq 7 \Rightarrow H < \ker \varepsilon$$

$$\Rightarrow \tilde{\varepsilon} : PSL(2,p) \cong PSL(2, \mathbb{Z}/p^e\mathbb{Z})/H \longrightarrow S_m$$

is well defined $\Rightarrow \tilde{\varepsilon} = 1 \Rightarrow \varepsilon = 1$

Let $N > 0$ $(N,2) = (N,3) = (N,5) = 1$

$$PSL(2, \mathbb{Z}/N\mathbb{Z}) \cong \bigoplus_{i=1}^{s} PSL(2, \mathbb{Z}/p_i^{\alpha_i}\mathbb{Z}) \qquad \varepsilon \text{ trivial.}$$

$$N = \prod_{i=1}^{s} p_i^{\alpha_i}$$

$$\begin{tikzcd} X(N) \arrow[d] \\ X(1) = \mathbb{P}^1(\mathbb{C}) \arrow[d] \\ X(N)^{Aut\, X(N)} \end{tikzcd} \qquad \begin{array}{ccc} \big|\,2 & \big|\,3 & N\,\big| \\ j(i) & j(\omega) & j(\infty) \end{array}$$

r = number of ram. points $r > 3 \Rightarrow$

$$|Aut\, X(N)| \leq 12(g_N - 1) \Rightarrow m \leq 1 \Rightarrow$$

$PSL(2, \mathbb{Z}/N\mathbb{Z}) \triangleleft Aut\, X(N)$.

$r=3$ ramification points

- $j(i)$, $j(\omega)$, $j(\infty)$ restrict to diff. points P_1, P_2, P_3

$1,\ q+1,\ q^d(q-1)$

$e(j(i)/P_1) = k$

$e(j(\omega)/P_2) = \lambda$

$e(j(\infty)/P_3) = \mu$ $\quad p^{t'}b$

$2(g_N-1) = |\mathrm{Aut}\,X(N)|\left(1-\frac{1}{2k}+1-\frac{1}{3\lambda}+1-\frac{1}{N\mu}-2\right) \geq$

$2g-2 = -2 + (q+1)p^t\alpha - \frac{(q+1)}{2}p^t\alpha + p^t - 1 \quad q^d p^{t'} b \frac{q}{1} - 1 + (q-1)$

$\geq |\mathrm{Aut}\,X(N)|\left(1-\frac{1}{2}+1-\frac{1}{3}+1-\frac{1}{N}-2\right) \geq$

$\geq |\mathrm{Aut}(X(N))|\left(\frac{1}{6}-\frac{1}{N}\right) = |\mathrm{Aut}\,X(N)|\,\frac{N-6}{6N} \Rightarrow$

$|\mathrm{Aut}(X(N))| \leq \frac{12N}{N-6}(g_N-1) = \mu N$

- $j(i)$ $\quad j(\infty)$ $\quad$ or $\quad j(\omega)$ $\quad j(\infty)$

k $\quad \lambda$

$\Rightarrow 2k = N\lambda$ $\quad$ but $\quad k \leq 6$, $\lambda \leq 6$ } imposible,

unless $N \leq 12 \Rightarrow m \leq 3 \Rightarrow N \leq 6$ contr. $N \geq 11$

Remark

$X(2)$, $X(4)$, $X(3)$, $X(5)$ rational curves

$PSL(2,2) \cong \mathbb{Z}_3$

$PSL(2, \mathbb{Z}/4\mathbb{Z}) \cong S_4$

$PSL(3,3) \cong A_4$

$PSL(2,5) \cong A_5$

A. Adler

$X(11)$ in char 3 $\longrightarrow M_{11}$

$q = p^t$, p prime

$F = \mathbb{F}_q(t)$, $A = \mathbb{F}_q[t]$ $F_\infty = \mathbb{F}_q((t^{-1}))$

C = completion of the algebraic closure of F_∞.

$\Omega = \mathbb{P}^1_C \setminus \mathbb{P}^1_{F_\infty} \xrightarrow[\text{acts}]{} GL(2,A)$

Z = center of $GL(2,A)$

$n \in A$.

$\Gamma(n) = \{ \gamma \in GL(2,A) : \gamma \equiv 1 \bmod n \}$

$\Omega / \Gamma(n)$ open analytic curve $\longrightarrow X(N)$

$$\begin{tikzcd} X(n) \arrow[d] \\ X(1) \cong \mathbb{P}^1 \end{tikzcd} \qquad \Big| \; q+1 \qquad \Big| \; q^d(q-1)$$

$d = \deg(n)$

$$g_{X(N)} - 1 = |G(n)| \frac{q^d - q - 1}{q^d (q^2 - 1)}$$

$$G(n) = \frac{\Gamma(1)}{\Gamma(n) Z}, \qquad |G(n)| = q^{3d} \prod_{p \mid n} \left(1 - \frac{1}{q^{2 \deg p}}\right)$$

$$|Aut(X(n))| \geq 84(g-1)$$

Problems

$\operatorname{char} k = 0$ $\quad |\mathrm{Aut}\, X| \leq 84(g-1)$

$\operatorname{char} k = p > 0$ $\quad |\mathrm{Aut}\, X| \leq f(g)$ $\quad \deg f = 4$

(one exep. $x^n + y^n + 1 = 0$ $\quad n = p^t + 1$)

Improved bounds

S. Nakajima

Ordinary curves

$$|\mathrm{Aut}(X)| \leq 84(g-1)g$$

Conjecture $\quad |\mathrm{Aut}(X)| \leq f(g)$ $\quad f = \frac{3}{2}$.

F. Kato. G. Cornelissen

Mumford curves

X is a Mumford curve, free group Γ on g-generators

a) X defined over a complete field k (non-Arch.)

b) $\mathcal{L}_\Gamma$: limit point set of Γ $\quad \mathrm{Aut}(X) = N/\Gamma$

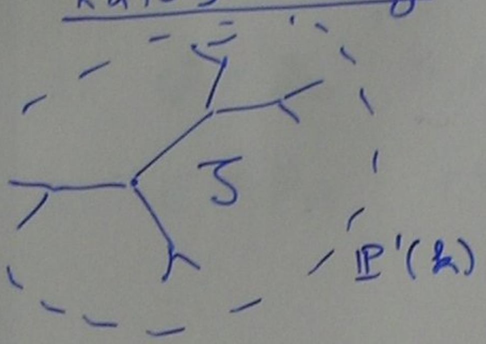
c) $X \cong \Gamma \backslash \mathbb{P}^1_k \setminus \mathcal{L}_\Gamma$

Herlich $\quad k = \mathbb{Q}_p \Rightarrow |\mathrm{Aut}\, X| \leq 12(g-1)$

Idea: Use analytic uniformization in order to prove Nakajima's conjecture for Mumford curves.

(2003 Guralnick - Zieve Anounced the proof of full Nakajima Conjecture)

Kato's theory



Bruhat-Tits Tree "bounded" by $\mathbb{P}^1(k)$

Definition of the trees $T_G : \mathcal{J}_G / G$

$T_G^* : \mathcal{J}_G^* / G$

$\mathcal{L}_N = \mathcal{L}_\Gamma \qquad \Omega = \mathbb{P}^1_K \setminus \mathcal{L}_N$

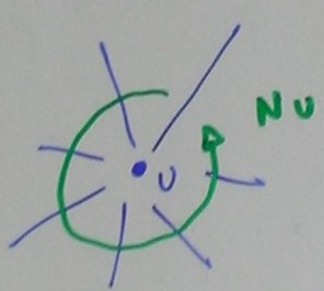
$$
\begin{array}{l}
\Omega \\
\downarrow \\
\Omega/\Gamma = X \\
\downarrow \\
\Omega/N = Y
\end{array}
\qquad \mathrm{Aut}(X)
$$

ramification points $\leftrightarrow$ ends $\mathcal{J}_N^*$ - ends $\mathcal{J}_N$

Branch points (X/Y) = ends T_N^*

T_N can be seen as a tree of groups (N_v stabilizer of a vertex).

N = tree product, N_v finite subgroups of $PGL(2, \mathbb{F}_q)$.



Finite groups of $PGL(2, \mathbb{F}_q)$:

1. $G = \mathbb{Z}_n$ $\quad (n, p) = 1 \quad d = 2, \quad G_1 = G_2 = \mathbb{Z}_n$

2. $G = D_n$ $\quad p \neq 2, \; n \mid p^m \pm 1 \quad d = 3 \quad G_1 = G_2 = \mathbb{Z}_2$
   $G_3 = \mathbb{Z}_n$

   or
   $p = 2 \quad (n, 2) = 1, \; d = 2 \quad G_1 = \mathbb{Z}_2$
   $G_2 = \mathbb{Z}_n$

3. $G = B(t, n)$ $\quad t \leq m \quad n \mid p^m - 1, \; n \mid p^t - 1$
   $d = 2 \quad G_1 = G, \; G_2 = \mathbb{Z}_n$ if $n > 1$
   $d = 1, \quad G_1 = G$ otherwise.
   $B(t, n) = E_t \rtimes \mathbb{Z}_n$

4. $G = P(2, p^t)$ $\quad d = 2 \quad G_1 = B(t, \{\tfrac{1}{2}\}(p^t - 1)), G_2 =$
   $\mathbb{Z}_{\{\frac{1}{2}\}(p^t + 1)}$

5. $G = A_4$ $\quad p \neq 2, 3 \quad d = 3$
   $G_1 = \mathbb{Z}_2, \; G_2 = G_3 = \mathbb{Z}_3$

6. $G = S_4$ $\quad p \neq 2, 3, \quad d = 3, \quad G_1 = \mathbb{Z}_2$
   $G_2 = G_3 = \mathbb{Z}_4$

7. $G = A_5$ $\quad 5 \mid p^{2m} - 1 \quad p \neq 2, 3, 5 \quad d = 3$
   $G_1 = \mathbb{Z}_2, G_2 = \mathbb{Z}_3, G_3 = \mathbb{Z}_5$

   or $p = 3, \; d = 2 \quad G_1 = B(1, 2), \; G_2 = \mathbb{Z}_5$

Stichtenoth: $|G| > 84(g-1) \Rightarrow$

$X \to X/G = \mathbb{P}^1$ and ramification at

2 or 3 points.

2 ram. points:

A1) $P(2,q) *_{B(t,n_-)} B(t_1,n_-)$ $n_\pm = \{\tfrac{1}{2}\}(q \pm 1)$

A2) $B(t_2,n_+) *_{\mathbb{Z}_{n_+}} P(2,q) *_{B(t,n_-)} B(t_1,n_-)$

A3) $B(t_3,n_-) *_{B(t,n_-)} P(2,q) *_{\mathbb{Z}_{n_+}} P(2,q) *_{B(t,n_-)} B(t_1,n_-)$

A4) $B(t_4,n_+) *_{\mathbb{Z}_{n_+}} P(2,q)$

A5) $B(t_5,n_-) *_{B(t,n_-)} P(2,q) *_{\mathbb{Z}_{n_+}} P(2,q)$

B) $B(t_1',n) *_{\mathbb{Z}_n} B(t_2',n)$

C) $E_{t_3'} * E_{t_4'}$

$N = PGL(?, q) *_{B(t, n-)} B(t_1, n)$

$t_1 = dt$

X

N contains N'

A1) on

$$B(t_3, n-) *_{B(t, n-)} P(2,q) * \mathbb{Z}_{\ast\ast} \; D_{\ast\ast} \; *_{\mathbb{Z}_2} Q(t_1) \; *_{\mathbb{Z}_2} Q(t_2)$$

$Q(t_i) = B(t_i, 2)$