Automorphism group of Cartan modular curves

Pietro Mercuri
a joint work with V. Dose and G. Lido

Sapienza Università di Roma

International Seminar on Automorphic Forms
16-01-2024

Modular curves as moduli spaces

Let n be a positive integer and let H be a subgroup of $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ containing $-I$, we associate a modular curve to H.

On the set of pairs (E, ϕ), where E is an elliptic curve and $\phi\colon (\mathbb{Z}/n\mathbb{Z})^2 \to E[n]$ is an isomorphism, we define the following equivalence relation:

$$(E,\phi) \sim_H (E',\phi') \iff \begin{array}{c}\text{there is an isomorphism } \iota\colon E \xrightarrow{\sim} E',\\ \text{and } (\phi')^{-1}\circ \iota|_{E[n]} \circ \phi \in H.\end{array}$$

$$\begin{tikzcd}
(\mathbb{Z}/n\mathbb{Z})^2 \arrow[r, "\phi"] \arrow[d, "(\phi')^{-1}\circ \iota|_{E[n]}\circ\phi"'] & E[n] \arrow[d, "\iota|_{E[n]}"] \\
(\mathbb{Z}/n\mathbb{Z})^2 \arrow[r, "\phi'"] & E'[n]
\end{tikzcd}$$

The modular curve Y_H is the coarse moduli space parametrizing $\{(E,\phi)\}/\sim_H$ and X_H is the compactification of Y_H. In particular, for every algebraically closed field K, there is a bijection between $Y_H(K)$ and $\{(E,\phi)\}/\sim_H$, where E is an elliptic curve over K.

Modular curves as moduli spaces

If $\det(H) = (\mathbb{Z}/n\mathbb{Z})^\times$, then Y_H and X_H are geometrically connected algebraic curves defined over $\mathbb{Q}$. Moreover, there are isomorphisms of Riemann surfaces

$$Y_H(\mathbb{C}) \cong \Gamma_H \backslash \mathcal{H} \qquad \text{and} \qquad X_H(\mathbb{C}) \cong \Gamma_H \backslash \mathcal{H}^*,$$

where $\mathcal{H} := \{z \in \mathbb{C} : \mathrm{Im}(z) > 0\}$ is the complex upper half-plane, $\mathcal{H}^* := \mathcal{H} \cup \mathbb{Q} \cup \{\infty\}$ is the extended complex upper half-plane,

$$\Gamma_H := \{\gamma \in \mathrm{SL}_2(\mathbb{Z}) : \gamma \pmod{n} \in H\},$$

is a congruence subgroup of level n and the action of $\mathrm{SL}_2(\mathbb{Z})$ on $\mathcal{H}^*$ is given, for $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$ and $\tau \in \mathcal{H}^*$, by

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \tau := \frac{a\tau + b}{c\tau + d}.$$

Examples

- When $H = \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$, we have $X_H = X(1) \cong \mathbb{P}^1$ (i.e., the j-line).

- When $H = B(n) := \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix}, a, d \in (\mathbb{Z}/n\mathbb{Z})^\times, b \in \mathbb{Z}/n\mathbb{Z} \right\}$ (the standard Borel subgroup), we have $X_H = X_0(n)$.

The action of Galois

Let K be a number field. There is an action of $\mathrm{Gal}(\bar{K}/K)$ on the points of Y_H.

If P is a point of Y_H given by $P = \{(E, \phi)\}/\sim_H$, then

$$P^\sigma := \{(E^\sigma, \phi^\sigma)\}/\sim_H, \qquad \text{for } \sigma \in \mathrm{Gal}(\bar{K}/K),$$

where:

- E^σ can be seen as the elliptic curve described by the same Weiestrass equation of E whose coefficients are the images under σ;
- $\phi^\sigma := \sigma \circ \phi$.

Rational points

Let K be a number field. A point on Y_H is *K-rational* if it is invariant with respect to $\mathrm{Gal}(\bar{K}/K)$, i.e., if

$$(E,\phi) \sim_H (E,\phi)^\sigma = (E^\sigma,\phi^\sigma), \qquad \text{for all } \sigma \in \mathrm{Gal}(\bar{K}/K),$$

that, using the description above, means

$$(E,\phi) \sim_H (E^\sigma,\phi^\sigma) \iff \begin{array}{c}\text{there is an isomorphism } \iota\colon E \xrightarrow{\sim} E^\sigma,\\ \text{and } (\phi^\sigma)^{-1}\circ \iota|_{E[n]}\circ\phi \in H.\end{array}$$

$$\begin{tikzcd}
(\mathbb{Z}/n\mathbb{Z})^2 \arrow[r, "\phi"] \arrow[d, "(\phi^\sigma)^{-1}\circ \iota|_{E[n]}\circ\phi"'] & E[n] \arrow[d, "\iota|_{E[n]}"] \\
(\mathbb{Z}/n\mathbb{Z})^2 \arrow[r, "\phi^\sigma"] & E^\sigma[n]
\end{tikzcd}$$

Rational points

Since E and E^σ are isomorphic for all $\sigma \in \mathrm{Gal}(\bar{K}/K)$ if and only if E is defined over K, then if a point $P = (E, \phi)$ of Y_H is K-rational, we have $E = E^\sigma$ and $\iota = \mathrm{id}_E$.

Hence we can state that $P = (E, \phi)$ is K-rational if and only if

- E is defined over K;
- $(\phi^\sigma)^{-1} \circ \iota|_{E[n]} \circ \phi = \phi^{-1} \circ \sigma^{-1} \circ \phi \in H$.

This can be rephrased as: $P = (E, \phi)$ is K-rational if and only if the image of the Galois representation (induced by the action of $\mathrm{Gal}(\bar{K}/K)$ on $E[n]$ via ϕ) associated to E is contained in H.

Rational points

One interesting problem is to determine the set of K-rational points of X_H for a number field K.

If the genus is at least 2, we know by Faltings Theorem that the number of K-rational points is finite. But we want to know precisely what they are.

This is hard even when $K = \mathbb{Q}$ and it is still an open problem although many improvements have been done.

Serre made a conjecture that describes the set of $\mathbb{Q}$-rational points $X_H(\mathbb{Q})$ when the level $n = p$ is prime.

Natural maps among modular curves

Since the natural maps $X_{H_1} \to X_{H_2}$, induced by the inclusions $H_1 \subset H_2$, are rationals, it is enough to study X_H when H is a proper maximal subgroup of $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$.

Example: Every modular curve X_H has a rational map toward the j-line $X(1) = X_{\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})}$, this map is called j-map.

Toward maximal subgroups of $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$

Let p be an odd prime and let ξ be a nonsquare modulo p, we define the following subgroups of $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$:

- the (standard) *split Cartan* subgroup
$$C_s(p) := \left\{ \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix}, a, d \in (\mathbb{Z}/p\mathbb{Z})^\times \right\};$$
- the normalizer of the (standard) split Cartan subroup
$$C_s^+(p) := C_s(p) \cup \left\{ \begin{pmatrix} 0 & b \\ c & 0 \end{pmatrix}, b, c \in (\mathbb{Z}/p\mathbb{Z})^\times \right\};$$
- the (standard) *nonsplit Cartan* subgroup
$$C_{ns}(p) := \left\{ \begin{pmatrix} a & b\xi \\ b & a \end{pmatrix}, a, b \in \mathbb{Z}/p\mathbb{Z}, (a, b) \not\equiv (0, 0) \bmod p \right\};$$
- the normalizer of the (standard) nonsplit Cartan subroup
$$C_{ns}^+(p) := C_{ns}(p) \cup \left\{ \begin{pmatrix} a & b\xi \\ -b & -a \end{pmatrix}, a, b \in \mathbb{Z}/p\mathbb{Z}, (a, b) \not\equiv (0, 0) \bmod p \right\}.$$

Cartan modular curves for prime levels

Correspondently we define the following modular curves:

$$X_{\mathrm{s}}(p) := X_{C_{\mathrm{s}}(p)}; \qquad X_{\mathrm{ns}}(p) := X_{C_{\mathrm{ns}}(p)};$$
$$X_{\mathrm{s}}^{+}(p) := X_{C_{\mathrm{s}}^{+}(p)}; \qquad X_{\mathrm{ns}}^{+}(p) := X_{C_{\mathrm{ns}}^{+}(p)}.$$

All of these are geometrically connected algebraic curves defined over $\mathbb{Q}$.

Moreover, if we define the following congruence subgroups of $\mathrm{SL}_2(\mathbb{Z})$:

$$\Gamma_{\mathrm{s}}(p) := \{\gamma \in \mathrm{SL}_2(\mathbb{Z}) : \gamma \pmod{p} \in C_{\mathrm{s}}(p)\};$$
$$\Gamma_{\mathrm{s}}^{+}(p) := \{\gamma \in \mathrm{SL}_2(\mathbb{Z}) : \gamma \pmod{p} \in C_{\mathrm{s}}^{+}(p)\};$$
$$\Gamma_{\mathrm{ns}}(p) := \{\gamma \in \mathrm{SL}_2(\mathbb{Z}) : \gamma \pmod{p} \in C_{\mathrm{ns}}(p)\};$$
$$\Gamma_{\mathrm{ns}}^{+}(p) := \{\gamma \in \mathrm{SL}_2(\mathbb{Z}) : \gamma \pmod{p} \in C_{\mathrm{ns}}^{+}(p)\}.$$

We have the following isomorphisms of Riemann surfaces:

$$X_{\mathrm{s}}(p)(\mathbb{C}) \cong \Gamma_{\mathrm{s}}(p)\backslash\mathcal{H}^*; \qquad X_{\mathrm{ns}}(p)(\mathbb{C}) \cong \Gamma_{\mathrm{ns}}(p)\backslash\mathcal{H}^*;$$
$$X_{\mathrm{s}}^{+}(p)(\mathbb{C}) \cong \Gamma_{\mathrm{s}}^{+}(p)\backslash\mathcal{H}^*; \qquad X_{\mathrm{ns}}^{+}(p)(\mathbb{C}) \cong \Gamma_{\mathrm{ns}}^{+}(p)\backslash\mathcal{H}^*.$$

Conjugate subgroups

If H_1 and H_2 are conjugate subgroups of $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$, then $X_{H_1} \cong X_{H_2}$.

This isomorphism is not modular! It is just an isomorphism of algebraic curves, but it is not compatible with the j-map.

Hence, every conjugate subgroup of $B(p)$, $C_{\mathrm{s}}(p)$, $C_{\mathrm{s}}^{+}(p)$, $C_{\mathrm{ns}}(p)$, $C_{\mathrm{ns}}^{+}(p)$ corresponds to a modular curve isomorphic to $X_0(p)$, $X_{\mathrm{s}}(p)$, $X_{\mathrm{s}}^{+}(p)$, $X_{\mathrm{ns}}(p)$, $X_{\mathrm{ns}}^{+}(p)$ respectively.

Maximal subgroups of $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$

Theorem

Let p be an odd prime and let H be a proper maximal subgroup of $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$ such that $\det(H) = (\mathbb{Z}/p\mathbb{Z})^\times$. Then, we can only have one of the following cases:

- *H is a Borel subgroup, i.e., it is a conjugate of $B(p)$;*
- *H is the normalizer of a split Cartan subgroup, i.e., it is a conjugate of $C_{\mathrm{s}}^+(p)$;*
- *H is the normalizer of a nonsplit Cartan subgroup, i.e., it is a conjugate of $C_{\mathrm{ns}}^+(p)$;*
- *H is an exceptional subgroup, i.e., its image in $\mathrm{PGL}_2(\mathbb{Z}/p\mathbb{Z})$ is isomorphic either to the symmetric group S_4 or to the alternating group A_4 or A_5.*

Expected rational points

Some rational points arise naturally, we call these points *expected rational points*.

The expected rational points can come only from cusps and from elliptic curves E with CM such that the class number of $\mathcal{O}_E$ is one. (An elliptic curve over $\mathbb{C}$ has Complex Multiplication if its endomorphism ring is isomorphic to an order $\mathcal{O}_E$ of an imaginary quadratic field.)

Expected rational points

The only 13 orders of an imaginary quadratic field with class number one are the orders with discriminant
$\Delta \in \{-3, -4, -7, -8, -11, -12, -16, -19, -27, -28, -43, -67, -163\}$.

The expected rational points are:

- If H is a Borel subgroup, the elliptic curves E as above such that p ramifies in $\mathcal{O}_E$ and the 2 cusps.
- If H is the normalizer of a split Cartan subgroup, the elliptic curves E as above such that p splits in $\mathcal{O}_E$ and 1 cusp (among the $\frac{1}{2}(p+1)$ cusps of the curve).
- If H is the normalizer of a nonsplit Cartan subgroup, the elliptic curves E as above such that p is inert in $\mathcal{O}_E$ (none of the $\frac{1}{2}(p-1)$ cusps of the curve is rational).
- If H is an exceptional subgroup, no rational point is expected.

Uniformity conjecture

Conjecture (Uniformity conjecture, Serre, 1972)

Let H_p be a maximal subgroup as above of the same type for every prime p. Then, there is a positive constant C such that the rational points of X_{H_p} are only the expected rational points for every $p > C$.

What is known?

- For the exceptional subgroups, this is true for $C = 13$.[a]
- For the Borel case, this is true for $C = 37$.[b]
- For the normalizer of a split Cartan subgroup, this is true for $C = 13$.[c]
- For the normalizer of a nonsplit Cartan subgroup, is this true?

[a] Serre, 1977
[b] Mazur, 1977
[c] Bilu, Parent, Rebolledo, 2013

Automorphisms

In some cases the knowledge of automorphism group helped to study the rational points.[d]

Let $\mathrm{GL}_2^+(\mathbb{Q}) := \{g \in \mathrm{GL}_2(\mathbb{Q}) : \det g > 0\}$ and let

$$\pi\colon \mathrm{GL}_2^+(\mathbb{Q}) \to \mathrm{PGL}_2^+(\mathbb{Q}) := \mathrm{GL}_2^+(\mathbb{Q})/\{\text{scalar matrices}\}$$

be the natural quotient map.

Each matrix $m \in \mathrm{PGL}_2^+(\mathbb{Q})$ defines a fractional linear transformation $m\colon \mathcal{H}^* \to \mathcal{H}^*$ and such an automorphism of the Riemann surface $\mathcal{H}^*$ pushes down to an automorphism of $\Gamma_H \backslash \mathcal{H}^*$ if and only if m normalizes $\pi(\Gamma_H)$.

Definition (Modular automorphisms)

If $\det(H) = (\mathbb{Z}/n\mathbb{Z})^\times$, an automorphism of X_H, defined over $\mathbb{C}$, is called *modular* if its action on $X_H(\mathbb{C}) = \Gamma_H \backslash \mathcal{H}^*$ is described by a fractional linear transformation of $\mathcal{H}^*$ associated to an element $m \in \mathrm{PGL}_2^+(\mathbb{Q})$ that normalizes $\pi(\Gamma_H)$ in $\mathrm{PGL}_2^+(\mathbb{Q})$.

[d] Kenku, 1981, and Momose, 1984

Automorphisms

Is every automorphism of X_H modular?

The answer is no when the genus is 0 or 1. It is not hard to see that in these cases there are non-modular automorphisms.

It is true for $X_0(n)$ when the genus is at least 2 and $n \neq 37, 63, 108$.[e,f,g,h]

[e] Ogg, 1977
[f] Kenku, Momose, 1988
[g] Elkies, 1990
[h] Harrison, 2011

Cartan groups for prime power levels

We can extend the previous Cartan groups to prime powers:

$$C_s(p^r) := \left\{ \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix}, a, d \in (\mathbb{Z}/p^r\mathbb{Z})^\times \right\};$$

$$C_s^+(p^r) := C_s(p^r) \cup \left\{ \begin{pmatrix} 0 & b \\ c & 0 \end{pmatrix}, b, c \in (\mathbb{Z}/p^r\mathbb{Z})^\times \right\};$$

$$C_{ns}(2^r) := \left\{ \begin{pmatrix} a & b \\ b & a+b \end{pmatrix}, a, b \in \mathbb{Z}/2^r\mathbb{Z}, (a, b) \not\equiv (0, 0) \bmod 2 \right\};$$

$$C_{ns}^+(2^r) := C_{ns}(2^r) \cup \left\{ \begin{pmatrix} a & a-b \\ b & -a \end{pmatrix}, a, b \in \mathbb{Z}/2^r\mathbb{Z}, (a, b) \not\equiv (0, 0) \bmod 2 \right\};$$

and for p odd and a nonsquare element $\xi \in (\mathbb{Z}/p^r\mathbb{Z})^\times$:

$$C_{ns}(p^r) := \left\{ \begin{pmatrix} a & b\xi \\ b & a \end{pmatrix}, a, b \in \mathbb{Z}/p^r\mathbb{Z}, (a, b) \not\equiv (0, 0) \bmod p \right\};$$

$$C_{ns}^+(p^r) := C_{ns}(p^r) \cup \left\{ \begin{pmatrix} a & b\xi \\ -b & -a \end{pmatrix}, a, b \in \mathbb{Z}/p^r\mathbb{Z}, (a, b) \not\equiv (0, 0) \bmod p \right\}.$$

Cartan modular curves for prime power levels

Correspondently we define the following modular curves:

$$X_{\mathrm{s}}(p^r) := X_{C_{\mathrm{s}}(p^r)}; \qquad X_{\mathrm{ns}}(p^r) := X_{C_{\mathrm{ns}}(p^r)};$$
$$X_{\mathrm{s}}^+(p^r) := X_{C_{\mathrm{s}}^+(p^r)}; \qquad X_{\mathrm{ns}}^+(p^r) := X_{C_{\mathrm{ns}}^+(p^r)}.$$

All of these are geometrically connected algebraic curves defined over $\mathbb{Q}$. If we define the following congruence subgroups of $\mathrm{SL}_2(\mathbb{Z})$:

$$\Gamma_{\mathrm{s}}(p^r) := \{\gamma \in \mathrm{SL}_2(\mathbb{Z}) : \gamma \pmod{p^r} \in C_{\mathrm{s}}(p^r)\};$$
$$\Gamma_{\mathrm{s}}^+(p^r) := \{\gamma \in \mathrm{SL}_2(\mathbb{Z}) : \gamma \pmod{p^r} \in C_{\mathrm{s}}^+(p^r)\};$$
$$\Gamma_{\mathrm{ns}}(p^r) := \{\gamma \in \mathrm{SL}_2(\mathbb{Z}) : \gamma \pmod{p^r} \in C_{\mathrm{ns}}(p^r)\};$$
$$\Gamma_{\mathrm{ns}}^+(p^r) := \{\gamma \in \mathrm{SL}_2(\mathbb{Z}) : \gamma \pmod{p^r} \in C_{\mathrm{ns}}^+(p^r)\}.$$

We have the following isomorphisms of Riemann surfaces:

$$X_{\mathrm{s}}(p^r)(\mathbb{C}) \cong \Gamma_{\mathrm{s}}(p^r)\backslash\mathcal{H}^*; \qquad X_{\mathrm{ns}}(p^r)(\mathbb{C}) \cong \Gamma_{\mathrm{ns}}(p^r)\backslash\mathcal{H}^*;$$
$$X_{\mathrm{s}}^+(p^r)(\mathbb{C}) \cong \Gamma_{\mathrm{s}}^+(p^r)\backslash\mathcal{H}^*; \qquad X_{\mathrm{ns}}^+(p^r)(\mathbb{C}) \cong \Gamma_{\mathrm{ns}}^+(p^r)\backslash\mathcal{H}^*.$$

Automorphisms of Cartan modular curves

Theorem (Dose, Lido, M., 2022)

If $p^r \notin \{2^3, 2^4, 2^5, 2^6, 3^2, 3^3, 11\}$, then all the automorphisms of the curves $X_{\mathrm{s}}(p^r), X_{\mathrm{s}}^+(p^r), X_{\mathrm{ns}}(p^r), X_{\mathrm{ns}}^+(p^r)$ with genus at least 2 are modular and

$$\mathrm{Aut}(X_{\mathrm{s}}(p^r)) \cong \begin{cases} (\mathbb{Z}/8\mathbb{Z})^2 \rtimes_\varphi (\mathbb{Z}/2\mathbb{Z}), & \text{if } p = 2, \\ \mathbb{Z}/3\mathbb{Z} \times S_3, & \text{if } p = 3, \\ \mathbb{Z}/2\mathbb{Z}, & \text{if } p > 3, \end{cases}$$

$$\mathrm{Aut}(X_{\mathrm{s}}^+(p^r)) \cong \begin{cases} \mathbb{Z}/8\mathbb{Z}, & \text{if } p = 2, \\ \mathbb{Z}/3\mathbb{Z}, & \text{if } p = 3, \\ \{1\}, & \text{if } p > 3, \end{cases}$$

$$\mathrm{Aut}(X_{\mathrm{ns}}(p^r)) \cong \mathbb{Z}/2\mathbb{Z},$$

$$\mathrm{Aut}(X_{\mathrm{ns}}^+(p^r)) \cong \{1\},$$

with $(\varphi(1))(x, y) = (y, x)$ and S_3 is the symmetric group acting on three elements.

Automorphisms of Cartan modular curves: exceptions

If $p^r \in \{2^3, 2^4, 2^5, 2^6, 3^2, 3^3, 11\}$, then is it true that all the automorphisms of the curves $X_s(p^r), X_s^+(p^r), X_{ns}(p^r), X_{ns}^+(p^r)$ are modular?

p^r	$X_s(p^r)$	$X_{ns}(p^r)$	$X_s^+(p^r)$	$X_{ns}^+(p^r)$
8	true $(g = 3)^i$	false $(g = 1)^j$	false $(g = 1)^j$	false $(g = 0)^j$
9	true $(g = 4)^i$	true $(g = 2)^k$	false $(g = 1)^j$	false $(g = 0)^j$
11	true $(g = 6)^i$	false $(g = 4)^l$	false $(g = 2)^m$	false $(g = 1)^j$
16	true $(g = 21)^i$	? $(g = 7)$	? $(g = 9)$	false $(g = 2)^k$
27	true $(g = 64)^i$	? $(g = 32)$	? $(g = 28)$	? $(g = 12)$
32	true $(g = 105)^{i,n}$	? $(g = 35)$	? $(g = 49)$	? $(g = 14)$
64	true $(g = 465)^{i,n}$	true $(g = 155)^n$	true $(g = 225)^n$	? $(g = 70)$

[i] Kenku, Momose, 1988

[j] Genus < 2

[k] Explicit computation using MAGMA

[l] Dose, Fernández, González, Schoof, 2014

[m] González, 2015

[n] Dose, Lido, M., 2022

Automorphisms of modular curves of Cartan type

Let $n \in \mathbb{Z}_{\geq 3}$ with prime factorization $n = \prod_{i=1}^{\omega(n)} p_i^{e_i}$ and let $H \cong \prod_{i=1}^{\omega(n)} H_{p_i}$ be a subgroup of $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$, where H_{p_i} is a subgroup of $\mathrm{GL}_2(\mathbb{Z}/p_i^{e_i}\mathbb{Z})$.

Theorem (Dose, Lido, M., 2022)

If $n \geq 10^{400}$ and H such that, for each $i = 1, \ldots, \omega(n)$, either $H_{p_i} \in \{C_{\mathrm{s}}(p_i^{e_i}), C_{\mathrm{ns}}(p_i^{e_i})\}$ or $H_{p_i} \in \{C_{\mathrm{s}}^+(p_i^{e_i}), C_{\mathrm{ns}}^+(p_i^{e_i})\}$, then every automorphism of X_H is modular and we have

$$\mathrm{Aut}(X_H) \cong \begin{cases} N'/H' \times \mathbb{Z}/2\mathbb{Z}, & \text{if } n \equiv 2 \bmod 4 \text{ and } H_2 = C_{\mathrm{s}}^+(2), \\ N'/H', & \text{otherwise,} \end{cases}$$

where $N' < \mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z})$ is the normalizer of $H' := H \cap \mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z})$.

Outline of the proof

Step 1. Prove, for the group $\mathrm{ModAut}(X_H)$ of modular automorphisms of X_H, that

$$\mathrm{ModAut}(X_H) \cong \begin{cases} N'/H' \times \mathbb{Z}/2\mathbb{Z}, & \text{if } n \equiv 2 \bmod 4 \text{ and } H_2 = C_s^+(2), \\ N'/H', & \text{otherwise,} \end{cases}$$

where $N' < \mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z})$ is the normalizer of $H' := H \cap \mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z})$.

Step 2. Prove that if there is a prime $\ell \nmid n$ such that $5 \leq \ell < \frac{1}{2}\mathrm{gon}(X_H) - 1$, where gon denotes the gonality, then each automorphism of X_H defined over a compositum of quadratic fields is modular.

Step 3. Apply the previous step, i.e., prove that such a prime ℓ exists.

Step 4. Prove that for $n \geq 10^{400}$, each automorphism is defined over a compositum of quadratic fields.

Step 1 (sketch)

Remind that $\pi\colon \mathrm{GL}_2^+(\mathbb{Q}) \to \mathrm{PGL}_2^+(\mathbb{Q})$ is the natural quotient map and $N' < \mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z})$ is the normalizer of $H' := H \cap \mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z})$.

Remark that if $\det(H) = (\mathbb{Z}/n\mathbb{Z})^\times$, the group of modular automorphisms is a subgroup of $\mathrm{Aut}(X_H)$ isomorphic to $N/\pi(\Gamma_H)$, where N is the normalizer of $\pi(\Gamma_H)$ in $\mathrm{PGL}_2^+(\mathbb{Q})$.

Some computations with groups of matrices show that $N = \pi(\Gamma_{N'})$ except in the special cases $n \equiv 2 \bmod 4$ and $H_2 = C_s^+(2)$.

Hence $N/\pi(\Gamma_H) = \pi(\Gamma_{N'})/\pi(\Gamma_H) = \pi(\Gamma_{N'})/\pi(\Gamma_{H'}) \cong N'/H'$.

In the remaining cases, we have that N is generated by $\pi(\Gamma_{N'})$ and one element that has order 2 in $N/\pi(\Gamma_H)$ and commutes with all the elements of N'/H'.

Hence $N/\pi(\Gamma_H) \cong N'/H' \times \mathbb{Z}/2\mathbb{Z}$.

Step 2 (sketch part a)

Prove that if there is a prime $\ell \nmid n$ such that $5 \leq \ell < \frac{1}{2}\mathrm{gon}(X_H) - 1$, then each automorphism of X_H defined over a compositum of quadratic fields is modular.

In order to show it we proved the following result describing the multiplicities of the points in the image of the Hecke operators T_ℓ.

Theorem

Let $\ell \geq 5$ be a prime not dividing n. We denote by $\rho = e^{\frac{2\pi i}{3}}$ and, for every $\tau \in \mathcal{H}$, we denote by E_τ the elliptic curve $\mathbb{C}/(\mathbb{Z} + \mathbb{Z}\tau)$. Then, for all points $P \in X_H(\mathbb{C})$, we have that:

1. *in $T_\ell(P)$ there is a point with multiplicity at least 4 if and only if P is a cusp;*
2. *in $T_\ell(P)$ there is a point with multiplicity 3 if and only if $P = (E_\rho, \phi)$ for some ϕ such that the matrix $\phi^{-1} \circ \rho|_{E_\rho[n]} \circ \phi$ lies in H (i.e., P is a branch point of X_H over $j(\rho) = 0$);*
3. *in $T_\ell(P)$ there are two distinct points with multiplicity 2 if and only if $P = (E_i, \phi)$ for some ϕ such that the matrix $\phi^{-1} \circ i|_{E_i[n]} \circ \phi$ lies in H (i.e., P is a branch point of X_H over $j(i) = 1728$).*

Step 2 (sketch part b)

Then we need the following commutation rule.

Theorem

Let $\ell \nmid n$ be a prime and let $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ be a Frobenius element at ℓ. Then, for any automorphism u of X_H defined over a compositum of quadratic fields, in $\mathrm{End}(\mathrm{Jac}(X_H))$

$$T_\ell \circ u = u^\sigma \circ T_\ell. \tag{1}$$

Moreover, if $\mathrm{gon}(X_H) > 2(\ell+1)$, then (1) holds at level of divisors.

The proof uses Eichler-Shimura relation modulo ℓ. The hypothesis on the definition field of u is used to get $\sigma^{-1} = \sigma$ and consequently remove the Frobenius morphism coming from Eichler-Shimura.

The condition $\mathrm{gon}(X_H) > 2(\ell+1)$ is used here to move from the Jacobian to actual divisors showing that the principal divisor $(T_\ell u - u^\sigma T_\ell)(P - Q)$, for $P, Q \in X_H(\mathbb{C})$, is in fact the zero divisor (there are no nonconstant rational functions with degree less than $2\ell+3$).

Step 2 (sketch part c)

Now, if we take an automorphism u of X_H, we can compare the multiplicities in the images of $T_\ell(P)$ and $T_\ell(u(P))$ for every point P of $X_H(\mathbb{C})$.

If u is defined over a compositum of quadratic fields, by the theorem of part b, we have that $T_\ell(u(P)) = u^\sigma(T_\ell(P))$.

Hence compare the multiplicities in the images of $T_\ell(P)$ and $T_\ell(u(P))$ is equivalent to compare the multiplicities in the images of $T_\ell(P)$ and $u^\sigma(T_\ell(P))$.

Since u^σ is an automorphism, it does not affect the multiplicities of $T_\ell(P)$. Hence the multiplicities of the two images of P under T_ℓ and $T_\ell u$ are the same. So the multiplicities in the images of P and $u(P)$ under T_ℓ are the same. Therefore, by the theorem of part a, we can conclude that u preserves the set of cusps and the set of branch points.

Hence we can conclude using the following result.

Theorem (Dose, 2016)

An automorphism of X_H is modular if and only if it preserves the set of cusps and the set of branch points

Step 3

We can apply the previous step because by Abramovich's bound we have

$$\mathrm{gon}(X_H) \geq \frac{7}{800}[\mathrm{SL}_2(\mathbb{Z}) : \Gamma_H] > 10n.$$

Hence, for every $n > 1$ there is a prime $\ell \nmid n$ such that $5 \leq \ell < 5n - 1$.

Step 4 (sketch part a)

Prove that for $n \geq 10^{400}$, each automorphism is defined over a compositum of quadratic fields.

As first step we extended a result of Kenku and Momose, 1988.

Theorem

Let K be a perfect field, let X be a smooth projective and geometrically connected curve over K of genus g and Jacobian variety J_X. If

- *there are two abelian varieties A_1 and A_2 over K such that $\mathrm{Hom}_{\overline{K}}(A_1, A_2) = 0$ and $J_X \sim_K A := A_1 \times_K A_2$;*
- $g > 2\dim(A_2) + 1$;
- *$F \subset \overline{K}$ is an extension of K such that $\mathrm{End}_{\overline{K}}(A_1) = \mathrm{End}_F(A_1)$.*

Then every automorphism of X over $\overline{K}$ can be defined over F.

Step 4 (sketch part a)

Theorem

Let K be a perfect field, let X be a smooth projective and geometrically connected curve over K of genus g and Jacobian variety J_X. If

- *there are two abelian varieties A_1 and A_2 over K such that $\mathrm{Hom}_{\overline{K}}(A_1, A_2) = 0$ and $J_X \sim_K A := A_1 \times_K A_2$;*
- *$g > 2\dim(A_2) + 1$;*
- *$F \subset \overline{K}$ is an extension of K such that $\mathrm{End}_{\overline{K}}(A_1) = \mathrm{End}_F(A_1)$.*

Then every automorphism of X over $\overline{K}$ can be defined over F.

In our case:

- $K = \mathbb{Q}$; $X = X_H$; F is a compositum of quadratic fields;
- A_2 is the CM part of J_X, i.e., the maximal abelian subvariety of J_X isogenous to a product of simple CM abelian varieties (a simple abelian variety A has CM if $\mathrm{End}_{\mathbb{Q}}(A)$ has degree $2\dim(A)$ over $\mathbb{Q}$ and is a totally imaginary quadratic extension of a totally real number field);
- A_1 is the non-CM part of J_X, i.e., the maximal abelian subvariety of J_X isogenous to a product of simple non-CM abelian varieties.

Step 4 (sketch part b)

Theorem

Let H be such that $H_{p_i} \in \{C_{\mathrm{s}}(p_i^{e_i}), C_{\mathrm{ns}}(p_i^{e_i})\}$ or $H_{p_i} \in \{C_{\mathrm{s}}^{+}(p_i^{e_i}), C_{\mathrm{ns}}^{+}(p_i^{e_i})\}$. Then J_H, the Jacobian of X_H, is a quotient of $J_0(n^2)$, the Jacobian of $X_0(n^2)$.

The split cases are well known and $C_{\mathrm{ns}}^{+}(p^r)$, with p odd, was already treated by Chen. Using Chen's ideas (i.e., essentially compute and compare characters of corresponding representations), we extended it to the remaining cases.

Corollary

J_H^{CM} is a quotient of $J_0(n^2)^{CM}$ and the non-CM part of J_H is a quotient of the non-CM part of $J_0(n^2)$.

Hence

$$2\dim(J_H^{\mathrm{CM}}) + 1 \leq 2\dim(J_0(n^2)^{\mathrm{CM}}) + 1.$$

Step 4 (sketch part c)

We bound the CM part of $J_0(n)$.

Theorem

For $n > 1$,

$$\dim J_0(n)^{CM} \leq 9\log(n)^2 n^{\frac{1}{2}+\frac{2.816}{\log\log n}}.$$

The proof relies on the following steps:

- Observe that $J_0(n)$ is isogenous to a product of abelian varieties A_f simple over $\mathbb{Q}$ associated to suitable newforms f.
- Observe (by Shimura) that the f contributing for the CM part are in bijection with triples $(K, \mathfrak{m}, \lambda)$, where K is an imaginary quadratic field with discriminant Δ_K, $\mathfrak{m}$ is an ideal of the ring of integers of K and λ is a primitive Grössencharacter of K defined modulo $\mathfrak{m}$ and such that $|\Delta_K||\mathfrak{m}|$ equal to the level of f.
- Give a bound on the number of these triples.

Step 4 (sketch part d)

Let g be the genus of X_H. For $n \geq 10^{400}$, we have

$$2\dim(J_H^{\mathrm{CM}}) + 1 \leq 2\dim(J_0(n^2)^{\mathrm{CM}}) + 1 \leq$$

$$\leq 73\log(n)^2 n^{1+\frac{5.632}{\log\log n}} < \frac{n^{2-\frac{0.96}{\log\log n}}}{100\log\log n} < g,$$

where:

- The first inequality comes from part b.
- The second inequality comes from part c.
- The last inequality follows giving bounds on the index $[\mathrm{SL}_2(\mathbb{Z}) : \Gamma_H]$, the number of elliptic points and cusps of X_H in the genus formula.

Finally we can conclude by part a, part b and the following result.

Theorem (Kenku, Momose, 1988)

Every endomorphism of the non-CM part of $J_0(n)$ is defined over the compositum of all the quadratic fields whose discriminant divides n.

THANK YOU!