,

Rational Points on Modular Jacobians

Elvira Lupoian

University of Warwick

19/4/2023

The Modular Curve $X_0(N)$

Fix a positive integer $N \geq 1$, and consider the congruence subgroup of $SL_2(\mathbb{Z})$

$$\Gamma_0(N) = \{\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in SL_2(\mathbb{Z}) \ : \ c \ \equiv \ 0 \bmod N\},$$

which acts on the upper half plane $\mathbb{H} = \{z \in \mathrm{C} \mid \mathrm{im}(z) > 0\}$ via fractional linear transformations

$$\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \cdot z = \frac{az+b}{cz+d} \text{ for any } \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_0(N) \text{ and } z \in \mathrm{H}.$$

and the quotient $Y_0(N) = \Gamma_0(N)/\mathbb{H}$ is a (non-compact) Riemann surface. We compactify this by adding finitely many points, called cusps

$$X_0(N) = Y_0(N) \cup \{\text{cusps}\}$$

so $X_0(N)$ is an compact Riemann surface, that is an algebraic curve.

Some Facts about $X_0(N)$

$$X_0(N) = \Gamma_0(N)/\mathbb{H}^* \text{ where}$$
$$\Gamma_0(N) = \{\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in SL_2(\mathbb{Z}) \ : \ c \equiv 0 \bmod N\},$$

- The algabraic curves $X_0(N)$ have models over $\mathbb{Q}$.

Some Facts about $X_0(N)$

$$X_0(N) = \Gamma_0(N)/\mathbb{H}^* \text{ where}$$
$$\Gamma_0(N) = \{\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in SL_2(\mathbb{Z}) \;:\; c \equiv 0 \bmod N\},$$

- The algabraic curves $X_0(N)$ have models over $\mathbb{Q}$.
- The cusps of $X_0(N)$ are in fact orbits of $\mathbb{P}^1(\mathbb{Q}) = \mathbb{Q} \cup \{\infty\}$, with the action of $\Gamma_0(N)$ extending to this in the natural way.

Some Facts about $X_0(N)$

$$X_0(N) = \Gamma_0(N)/\mathbb{H}^* \text{ where}$$
$$\Gamma_0(N) = \{\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in SL_2(\mathbb{Z}) \;:\; c \equiv 0 \bmod N\},$$

- The algabraic curves $X_0(N)$ have models over $\mathbb{Q}$.
- The cusps of $X_0(N)$ are in fact orbits of $\mathbb{P}^1(\mathbb{Q}) = \mathbb{Q} \cup \{\infty\}$, with the action of $\Gamma_0(N)$ extending to this in the natural way.
- Non-cuspidal points of $X_0(N)$ are in natural bijection with isomorphism classes $[E, C]$, where E is an elliptic curve and C is a degree N cyclic subgroup of $E[N]$.

$$X_0(N)(K) \leftrightarrow \{[E/K, 0 \neq C \subsetneq E[N]]\}$$

Some Facts about $X_0(N)$

$$X_0(N) = \Gamma_0(N)/\mathbb{H}^* \text{ where}$$
$$\Gamma_0(N) = \{\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in SL_2(\mathbb{Z}) \ : \ c \ \equiv \ 0 \bmod N\},$$

- The algabraic curves $X_0(N)$ have models over $\mathbb{Q}$.
- The cusps of $X_0(N)$ are in fact orbits of $\mathbb{P}^1(\mathbb{Q}) = \mathbb{Q} \cup \{\infty\}$, with the action of $\Gamma_0(N)$ extending to this in the natural way.
- Non-cuspidal points of $X_0(N)$ are in natural bijection with isomorphism classes $[E, C]$, where E is an elliptic curve and C is a degree N cyclic subgroup of $E[N]$.

$$X_0(N)(K) \leftrightarrow \{[E/K, 0 \neq C \subsetneq E[N]]\}$$

Naive Approach

One can derive equations for these curves and sometimes solve directly for rational points.

Naive Approach

One can derive equations for these curves and sometimes solve directly for rational points.
For example the curve $X_0(83)$ has genus 7, it is non-hyperelliptic curve, and its cut out in $\mathbb{P}^6$ by 10 quadrics.

Naive Approach

One can derive equations for these curves and sometimes solve directly for rational points.
For example the curve $X_0(83)$ has genus 7, it is non-hyperelliptic curve, and its cut out in $\mathbb{P}^6$ by 10 quadrics.

$$x_1x_3 - x_2^2 - 2x_4x_5 - x_4x_7 - 5/2x_5^2 + 5x_5x_6 + 1/2x_5x_7 - 3/2x_6^2 - 9/2x_6x_7 - 13/2x_7^2,$$

$$x_1x_4 - x_2x_3 - x_3x_6 - 3x_4x_5 + 3x_4x_6 + 3x_4x_7 - 7/2x_5^2 + 9x_5x_6 + 5/2x_5x_7 - 11/2x_6^2 - 29/2x_6x_7 - 25/2x_7^2$$

$$x_1x_5 - x_2x_6 - x_3^2 + 3x_3x_6 + x_4^2 - 3x_4x_5 - 2x_4x_6 - 1/2x_4x_7 + 17/4x_5^2 - 5/2x_5x_6 - 35/4x_5x_7 + 5/4x_6^2 + 27/4x_6x_7 + 23/4x_7^2$$

$$x_1x_6 - x_2x_6 - x_3x_4 + x_3x_6 + x_4^2 - 4x_4x_5 + x_4x_6 + 5/2x_4x_7 + 1/4x_5^2 + 11/2x_5x_6 - 11/4x_5x_7 - 11/4x_6^2 - 21/4x_6x_7 - 13/4x_7^2$$

X_0 (83)

$$x_1x_7 - x_4^2 + 2x_4x_5 + 2x_4x_6 - x_5^2 - 2x_5x_6 + 2x_5x_7 - x_6^2$$

$$x_2x_4 - 2x_2x_6 - x_3^2 + 4x_3x_6 + 2x_4^2 - 4x_4x_5 - 5x_4x_6 - x_4x_7 + 7x_5^2 - 6x_5x_6 - 14x_5x_7 + 5x_6^2 + 16x_6x_7 + 15x_7^2$$

$$x_2x_5 - x_2x_6 - x_3x_4 + 2x_3x_6 + x_4^2 - 2x_4x_5 + 2x_4x_7 + 3x_5^2 - 3x_5x_6 - 8x_5x_7 + 4x_6x_7 + 6x_7^2$$

$$x_2x_7 - x_4x_5 + x_4x_6 + x_4x_7 + x_5^2 - 2x_5x_7 - x_6^2 - x_6x_7$$

$$x_3x_5 - x_3x_6 - x_4^2 + x_4x_5 + 3x_4x_6 + x_4x_7 - 3x_5^2 + 2x_5x_6 + 5x_5x_7 - 3x_6^2 - 7x_6x_7 - 6x_7^2$$

$$x_3x_7 - x_5^2 + 2x_5x_6 + 2x_5x_7 - x_6^2 - 4x_6x_7 - 3x_7^2$$

An Alternative Approach

From now on, we will only use the modular properties of the curve. Using specific equations describing our curves will be against the rules! We will make use of the following

An Alternative Approach

From now on, we will only use the modular properties of the curve. Using specific equations describing our curves will be against the rules! We will make use of the following

- The cusps are easily accessible and can be computed efficiently.

An Alternative Approach

From now on, we will only use the modular properties of the curve. Using specific equations describing our curves will be against the rules! We will make use of the following

- The cusps are easily accessible and can be computed efficiently.
- The rational cusps generate large finite groups of rational divisors of degree 0, that is subgroups of $J_0(N)(\mathbb{Q})$, where $J_0(N)$ is the Jacobian of $X_0(N)$.

An Alternative Approach

From now on, we will only use the modular properties of the curve. Using specific equations describing our curves will be against the rules! We will make use of the following

- The cusps are easily accessible and can be computed efficiently.
- The rational cusps generate large finite groups of rational divisors of degree 0, that is subgroups of $J_0(N)(\mathbb{Q})$, where $J_0(N)$ is the Jacobian of $X_0(N)$.
- For some values of N, we can determine $X_0(N)(\mathbb{Q})$ from $J_0(N)(\mathbb{Q})$.

An Alternative Approach

From now on, we will only use the modular properties of the curve. Using specific equations describing our curves will be against the rules! We will make use of the following

- The cusps are easily accessible and can be computed efficiently.
- The rational cusps generate large finite groups of rational divisors of degree 0, that is subgroups of $J_0(N)(\mathbb{Q})$, where $J_0(N)$ is the Jacobian of $X_0(N)$.
- For some values of N, we can determine $X_0(N)(\mathbb{Q})$ from $J_0(N)(\mathbb{Q})$.

Denote by $C_0(N)$ the subgroup of $J_0(N)$ generated by differences of cusps. We refer to this as the cuspidal subgroup.

An Alternative Approach

From now on, we will only use the modular properties of the curve. Using specific equations describing our curves will be against the rules! We will make use of the following

- The cusps are easily accessible and can be computed efficiently.
- The rational cusps generate large finite groups of rational divisors of degree 0, that is subgroups of $J_0(N)(\mathbb{Q})$, where $J_0(N)$ is the Jacobian of $X_0(N)$.
- For some values of N, we can determine $X_0(N)(\mathbb{Q})$ from $J_0(N)(\mathbb{Q})$.

Denote by $C_0(N)$ the subgroup of $J_0(N)$ generated by differences of cusps. We refer to this as the cuspidal subgroup. Theorems of Manin and Drinfeld tell us that points of $C_0(N)$ are torsion points and thus

$$C_0(N)(\mathbb{Q}) \subseteq J_0(N)(\mathbb{Q})_{\text{tors}}$$

where $J_0(N)(\mathbb{Q}) \cong J_0(N)(\mathbb{Q})_{\text{tors}} \times \mathbb{Z}^r$, since $J_0(N)$ is an abelian variety.

Prime Level Case

For a prime $p \geq 5$, the modular curve $X_0(p)$ has two cups, which we denote by 0 and ∞, and both are rational. In 1973, Ogg proved the following.

Prime Level Case

For a prime $p \geq 5$, the modular curve $X_0(p)$ has two cups, which we denote by 0 and ∞, and both are rational. In 1973, Ogg proved the following.

Proposition (Ogg)

The cuspidal subgroup $C_0(p)$ is a cyclic group of order the numerator of $\frac{p-1}{12}$.

Prime Level Case

For a prime $p \geq 5$, the modular curve $X_0(p)$ has two cups, which we denote by 0 and ∞, and both are rational. In 1973, Ogg proved the following.

Proposition (Ogg)

The cuspidal subgroup $C_0(p)$ is a cyclic group of order the numerator of $\frac{p-1}{12}$.

In 1977, in his celebrated paper " Modular Curves and the Eisenstein ideal", Mazur proved that the trivial containment

$$C_0(N)(\mathbb{Q}) \subseteq J_0(N)(\mathbb{Q})_{\text{tors}}$$

is in fact an equality!

Prime Level Case

For a prime $p \geq 5$, the modular curve $X_0(p)$ has two cups, which we denote by 0 and ∞, and both are rational. In 1973, Ogg proved the following.

Proposition (Ogg)

The cuspidal subgroup $C_0(p)$ is a cyclic group of order the numerator of $\frac{p-1}{12}$.

In 1977, in his celebrated paper " Modular Curves and the Eisenstein ideal", Mazur proved that the trivial containment

$$C_0(N)(\mathbb{Q}) \subseteq J_0(N)(\mathbb{Q})_{\text{tors}}$$

is in fact an equality!

Theorem (Mazur)

For a prime $p \geq 5$,

$$C_0(p)(\mathbb{Q}) = J_0(p)(\mathbb{Q})_{tors} \cong C_k$$

where k is the numerator of $\frac{p-1}{12}$.

The Generalized Ogg Conjecture

For a composite N, we may conjecture the following.

Conjecture (The Generalized Ogg Conjecture)

For an integer $N \geq 5$, $C_0(N)(\mathbb{Q}) = J_0(N)(\mathbb{Q})_{tors}$

The Generalized Ogg Conjecture

For a composite N, we may conjecture the following.

Conjecture (The Generalized Ogg Conjecture)

For an integer $N \geq 5$, $C_0(N)(\mathbb{Q}) = J_0(N)(\mathbb{Q})_{tors}$

There has been much progress towards proving this conjecture in recent years.

- Explicit computations by Ligozat for $N \in \{11, 14, , 15, 17, 19, 20, 21, 24, 27, 32, 36, 49\}$ (1975)

The Generalized Ogg Conjecture

For a composite N, we may conjecture the following.

Conjecture (The Generalized Ogg Conjecture)

For an integer $N \geq 5$, $C_0(N)(\mathbb{Q}) = J_0(N)(\mathbb{Q})_{tors}$

There has been much progress towards proving this conjecture in recent years.

- Explicit computations by Ligozat for $N \in \{11, 14, , 15, 17, 19, 20, 21, 24, 27, 32, 36, 49\}$ (1975)
- Explicit computations for $N \in \{34, 38, 44, 45, 51, 52, 54, 56, 64, 82\}$ by Ozman and Siksek (2019); and for $N \in \{57, 65\}$ by Box (2019)

The Generalized Ogg Conjecture

For a composite N, we may conjecture the following.

Conjecture (The Generalized Ogg Conjecture)

For an integer $N \geq 5$, $C_0(N)(\mathbb{Q}) = J_0(N)(\mathbb{Q})_{tors}$

There has been much progress towards proving this conjecture in recent years.

- Explicit computations by Ligozat for $N \in \{11, 14, , 15, 17, 19, 20, 21, 24, 27, 32, 36, 49\}$ (1975)
- Explicit computations for $N \in \{34, 38, 44, 45, 51, 52, 54, 56, 64, 82\}$ by Ozman and Siksek (2019); and for $N \in \{57, 65\}$ by Box (2019)
- Ribet, Kenneth and Wake (2022) proved that for a square-free N and any prime $p \nmid 6N$, the p-primary parts of $J_0(N)(\mathbb{Q})_{\text{tors}}$ and $C_N(\mathbb{Q})$ coincide

The Generalized Ogg Conjecture

For a composite N, we may conjecture the following.

Conjecture (The Generalized Ogg Conjecture)

For an integer $N \geq 5$, $C_0(N)(\mathbb{Q}) = J_0(N)(\mathbb{Q})_{tors}$

There has been much progress towards proving this conjecture in recent years.

- Explicit computations by Ligozat for $N \in \{11, 14, , 15, 17, 19, 20, 21, 24, 27, 32, 36, 49\}$ (1975)
- Explicit computations for $N \in \{34, 38, 44, 45, 51, 52, 54, 56, 64, 82\}$ by Ozman and Siksek (2019); and for $N \in \{57, 65\}$ by Box (2019)
- Ribet, Kenneth and Wake (2022) proved that for a square-free N and any prime $p \nmid 6N$, the p-primary parts of $J_0(N)(\mathbb{Q})_{\text{tors}}$ and $C_N(\mathbb{Q})$ coincide
- Many other results of this kind have been proved by Yoo (2019), Wang and Yang (2020), Ren (2018) and many others

Other Modular Curves

The points of the modular curve $X_1(N) \cong \Gamma_1(N)/\mathbb{H}^*$ parametrize (isomorphism classes) of elliptic curves with an N-torsion points,

$$\Gamma_1(N) = \{\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in SL_2(\mathbb{Z}) \ : \ a, c \ 1 \bmod N \text{ and } c \ \equiv \ 0 \bmod N\}$$

Other Modular Curves

The points of the modular curve $X_1(N) \cong \Gamma_1(N)/\mathbb{H}^*$ parametrize (isomorphism classes) of elliptic curves with an N-torsion points,

$$\Gamma_1(N) = \{\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in SL_2(\mathbb{Z}) \ : \ a, c\ 1 \bmod N \text{ and } c \ \equiv \ 0 \bmod N\}$$

- In 2011 Stein showed that $J_1(p)(\mathbb{Q})_{\text{tors}}$ is cuspidal $p \leq 157$, except possibly for $29, 97, 101, 109, 113$

Other Modular Curves

The points of the modular curve $X_1(N) \cong \Gamma_1(N)/\mathbb{H}^*$ parametrize (isomorphism classes) of elliptic curves with an N-torsion points,

$$\Gamma_1(N) = \{\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in SL_2(\mathbb{Z}) \ : \ a, c \ 1 \bmod N \text{ and } c \ \equiv \ 0 \bmod N\}$$

- In 2011 Stein showed that $J_1(p)(\mathbb{Q})_{\text{tors}}$ is cuspidal $p \leq 157$, except possibly for $29, 97, 101, 109, 113$
- The genus of these curves grows extremely fast, and in general computations with these curves are difficult.

Other Modular Curves

The points of the modular curve $X_1(N) \cong \Gamma_1(N)/\mathbb{H}^*$ parametrize (isomorphism classes) of elliptic curves with an N-torsion points,

$$\Gamma_1(N) = \{\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in SL_2(\mathbb{Z}) \;:\; a, c \; 1 \bmod N \text{ and } c \;\equiv\; 0 \bmod N\}$$

- In 2011 Stein showed that $J_1(p)(\mathbb{Q})_{\text{tors}}$ is cuspidal $p \leq 157$, except possibly for $29, 97, 101, 109, 113$
- The genus of these curves grows extremely fast, and in general computations with these curves are difficult.

There is also the analogous question asked by Mar for generalized Jacobians, and the analogoues results for l-primary parts.

$X_H(p)$

Fix a prime $p \geq 5$, and take $H \leq (\mathbb{Z}/p\mathbb{Z})^*$ any subgroup.

$X_H(p)$

Fix a prime $p \geq 5$, and take $H \leq (\mathbb{Z}/p\mathbb{Z})^*$ any subgroup. We define the congruence subgroup

$$\Gamma_H(p) = \{\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in SL_2(\mathbb{Z}) \ : \ a, d \bmod p \ \in H, \ c \ \equiv \ 0 \bmod p\},$$

$X_H(p)$

Fix a prime $p \geq 5$, and take $H \leq (\mathbb{Z}/p\mathbb{Z})^*$ any subgroup. We define the congruence subgroup

$$\Gamma_H(p) = \{\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in SL_2(\mathbb{Z}) \ : \ a, d \bmod p \ \in H, \ c \ \equiv \ 0 \bmod p\},$$

and as before this group acts on the upper half plane and the quotient $Y_H(p) = \Gamma_H(p)/\mathbb{H}$ is a Riemann surface, which can be compactified, by adding finitely many cusps, to obtain

$X_H(p)$

Fix a prime $p \geq 5$, and take $H \leq (\mathbb{Z}/p\mathbb{Z})^*$ any subgroup. We define the congruence subgroup

$$\Gamma_H(p) = \{\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in SL_2(\mathbb{Z}) \ : \ a, d \bmod p \ \in H, \ c \ \equiv \ 0 \bmod p\},$$

and as before this group acts on the upper half plane and the quotient $Y_H(p) = \Gamma_H(p)/\mathbb{H}$ is a Riemann surface, which can be compactified, by adding finitely many cusps, to obtain

$$X_H(p) = Y_H(p) \cup \{\text{cusps}\}$$

$X_H(p)$

Fix a prime $p \geq 5$, and take $H \leq (\mathbb{Z}/p\mathbb{Z})^*$ any subgroup. We define the congruence subgroup

$$\Gamma_H(p) = \{\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in SL_2(\mathbb{Z}) \ : \ a, d \bmod p \ \in H, \ c \ \equiv \ 0 \bmod p\},$$

and as before this group acts on the upper half plane and the quotient $Y_H(p) = \Gamma_H(p)/\mathbb{H}$ is a Riemann surface, which can be compactified, by adding finitely many cusps, to obtain

$$X_H(p) = Y_H(p) \cup \{\text{cusps}\}$$

so $X_H(p)$ is an compact Riemann surface, that is an algebraic curve.

$X_H(p)$

Fix a prime $p \geq 5$, and take $H \leq (\mathbb{Z}/p\mathbb{Z})^*$ any subgroup. We define the congruence subgroup

$$\Gamma_H(p) = \{\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in SL_2(\mathbb{Z}) \ : \ a, d \bmod p \ \in H, \ c \ \equiv \ 0 \bmod p\},$$

and as before this group acts on the upper half plane and the quotient $Y_H(p) = \Gamma_H(p)/\mathbb{H}$ is a Riemann surface, which can be compactified, by adding finitely many cusps, to obtain

$$X_H(p) = Y_H(p) \cup \{\text{cusps}\}$$

so $X_H(p)$ is an compact Riemann surface, that is an algebraic curve.

- As before, $X_H(p)$ has a model over $\mathbb{Q}$.

$X_H(p)$

Fix a prime $p \geq 5$, and take $H \leq (\mathbb{Z}/p\mathbb{Z})^*$ any subgroup. We define the congruence subgroup

$$\Gamma_H(p) = \{\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in SL_2(\mathbb{Z}) \ : \ a, d \bmod p \ \in H, \ c \ \equiv \ 0 \bmod p\},$$

and as before this group acts on the upper half plane and the quotient $Y_H(p) = \Gamma_H(p)/\mathbb{H}$ is a Riemann surface, which can be compactified, by adding finitely many cusps, to obtain

$$X_H(p) = Y_H(p) \cup \{\text{cusps}\}$$

so $X_H(p)$ is an compact Riemann surface, that is an algebraic curve.

- As before, $X_H(p)$ has a model over $\mathbb{Q}$.
- Taking $H = 1$, we obtain $X_1(p)$

$X_H(p)$

Fix a prime $p \geq 5$, and take $H \leq (\mathbb{Z}/p\mathbb{Z})^*$ any subgroup. We define the congruence subgroup

$$\Gamma_H(p) = \{\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in SL_2(\mathbb{Z}) \ : \ a, d \bmod p \ \in H, \ c \ \equiv \ 0 \bmod p\},$$

and as before this group acts on the upper half plane and the quotient $Y_H(p) = \Gamma_H(p)/\mathbb{H}$ is a Riemann surface, which can be compactified, by adding finitely many cusps, to obtain

$$X_H(p) = Y_H(p) \cup \{\text{cusps}\}$$

so $X_H(p)$ is an compact Riemann surface, that is an algebraic curve.

- As before, $X_H(p)$ has a model over $\mathbb{Q}$.
- Taking $H = 1$, we obtain $X_1(p)$
- ... and $H = (\mathbb{Z}/p\mathbb{Z})^*$ gives $X_0(p)$

$X_H(p)$

Fix a prime $p \geq 5$, and take $H \leq (\mathbb{Z}/p\mathbb{Z})^*$ any subgroup. We define the congruence subgroup

$$\Gamma_H(p) = \{\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in SL_2(\mathbb{Z}) \ : \ a, d \bmod p \ \in H, \ c \ \equiv \ 0 \bmod p\},$$

and as before this group acts on the upper half plane and the quotient $Y_H(p) = \Gamma_H(p)/\mathbb{H}$ is a Riemann surface, which can be compactified, by adding finitely many cusps, to obtain

$$X_H(p) = Y_H(p) \cup \{\text{cusps}\}$$

so $X_H(p)$ is an compact Riemann surface, that is an algebraic curve.

- As before, $X_H(p)$ has a model over $\mathbb{Q}$.
- Taking $H = 1$, we obtain $X_1(p)$
- ... and $H = (\mathbb{Z}/p\mathbb{Z})^*$ gives $X_0(p)$

The natural quotient maps give the following maps between the curves

$$X_0(p) \leftarrow X_H(p) \leftarrow X_1(p)$$

Moduli Interpretation

$$X_H(p) = Y_H(p) \cup \{\text{cusps}\}$$

$$\Gamma_H(p) = \{\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in SL_2(\mathbb{Z}) \ : \ a, d \bmod p \in H, \ c \equiv 0 \bmod p\},$$

Moduli Interpretation

$$X_H(p) = Y_H(p) \cup \{\text{cusps}\}$$

$$\Gamma_H(p) = \{\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in SL_2(\mathbb{Z}) \;:\; a, d \bmod p \in H,\; c \equiv 0 \bmod p\},$$

The non-cuspidal points of $X_H(p)$ correspond to isomorphism classes of elliptic curves with H-level structure, but we can alternatively think of these as elliptic curves whose image of the Galois representation is (up to conjugation)

Moduli Interpretation

$$X_H(p) = Y_H(p) \cup \{\text{cusps}\}$$

$$\Gamma_H(p) = \{\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in SL_2(\mathbb{Z}) \ : \ a, d \bmod p \ \in H, \ c \ \equiv \ 0 \bmod p\},$$

The non-cuspidal points of $X_H(p)$ correspond to isomorphism classes of elliptic curves with H-level structure, but we can alternatively think of these as elliptic curves whose image of the Galois representation is (up to conjugation)

$$\begin{pmatrix} * \in H & * \\ 0 & * \end{pmatrix}$$

Moduli Interpretation

$$X_H(p) = Y_H(p) \cup \{\text{cusps}\}$$

$$\Gamma_H(p) = \{\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in SL_2(\mathbb{Z}) \ : \ a, d \bmod p \ \in H, \ c \ \equiv \ 0 \bmod p\},$$

The non-cuspidal points of $X_H(p)$ correspond to isomorphism classes of elliptic curves with H-level structure, but we can alternatively think of these as elliptic curves whose image of the Galois representation is (up to conjugation)

$$\begin{pmatrix} * \in H & * \\ 0 & * \end{pmatrix}$$

- As before, the cups are accessible

Moduli Interpretation

$$X_H(p) = Y_H(p) \cup \{\text{cusps}\}$$

$$\Gamma_H(p) = \{\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in SL_2(\mathbb{Z}) \ : \ a, d \bmod p \ \in H, \ c \ \equiv \ 0 \bmod p\},$$

The non-cuspidal points of $X_H(p)$ correspond to isomorphism classes of elliptic curves with H-level structure, but we can alternatively think of these as elliptic curves whose image of the Galois representation is (up to conjugation)

$$\begin{pmatrix} * \in H & * \\ 0 & * \end{pmatrix}$$

- As before, the cups are accessible
- We define the cuspidal subgroup $C_H(p) \subset J_H(p)$, which consists of torsion points; and hence $C_H(p)(\mathbb{Q}) \subset J_H(p)(\mathbb{Q})_{\text{tors}}$

Moduli Interpretation

$$X_H(p) = Y_H(p) \cup \{\text{cusps}\}$$

$$\Gamma_H(p) = \{\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in SL_2(\mathbb{Z}) \ : \ a, d \bmod p \ \in H, \ c \ \equiv \ 0 \bmod p\},$$

The non-cuspidal points of $X_H(p)$ correspond to isomorphism classes of elliptic curves with H-level structure, but we can alternatively think of these as elliptic curves whose image of the Galois representation is (up to conjugation)

$$\begin{pmatrix} * \in H & * \\ 0 & * \end{pmatrix}$$

- As before, the cups are accessible
- We define the cuspidal subgroup $C_H(p) \subset J_H(p)$, which consists of torsion points; and hence $C_H(p)(\mathbb{Q}) \subset J_H(p)(\mathbb{Q})_{\text{tors}}$
- Is the above containment ever an equality?

$X_H(p)$

Let $p \geq 5$ be prime and congruent to 1 modulo 4, and we take H to be the subgroup of non-zero squares modulo p. The quotient map induces a degree 2 map

$$X_0(p) \longleftarrow X_H(p)$$

and using this map in computations, we may deduce the following.

$X_H(p)$

Let $p \geq 5$ be prime and congruent to 1 modulo 4, and we take H to be the subgroup of non-zero squares modulo p. The quotient map induces a degree 2 map

$$X_0(p) \longleftarrow X_H(p)$$

and using this map in computations, we may deduce the following.

Theorem

With notation as above, for all p such that the genus of $g = X_H(p)$ is $2 \leq g \leq 10$, we have

$$C_H(p)(\mathbb{Q}) = J_H(p)(\mathbb{Q})_{tors}$$

$X_H(p)$

Let $p \geq 5$ be prime and congruent to 1 modulo 4, and we take H to be the subgroup of non-zero squares modulo p. The quotient map induces a degree 2 map

$$X_0(p) \longleftarrow X_H(p)$$

and using this map in computations, we may deduce the following.

Theorem

With notation as above, for all p such that the genus of $g = X_H(p)$ is $2 \leq g \leq 10$, we have

$$C_H(p)(\mathbb{Q}) = J_H(p)(\mathbb{Q})_{tors}$$

Moreover, $C_H(p) \cong (\mathbb{Z}/n\mathbb{Z}) \times (\mathbb{Z}/m\mathbb{Z})$, where $n, m \in \mathbb{Z}$ and m is the lowest common multiple of n and the numerator of $\frac{p-1}{12}$; and the rational part is $C_H(p)(\mathbb{Q}) \cong (\mathbb{Z}/m\mathbb{Z})$.

$J_H(p)\left(\mathbb{Q}\left(\sqrt{p}\right)\right)_{\text{tors}}$

Taking $H = \{a^2 \ : \ a \in (\mathbb{Z}/p\mathbb{Z})^*\}$, where p is prime congruent to 1 modulo 4, the cusps of $X_H(p)$ are defined over $\mathbb{Q}\left(\sqrt{p}\right)$ and Galois conjugate.

$J_H(p)\left(\mathbb{Q}\left(\sqrt{p}\right)\right)_{\text{tors}}$

Taking $H = \{a^2 \;:\; a \in (\mathbb{Z}/p\mathbb{Z})^*\}$, where p is prime congruent to 1 modulo 4, the cusps of $X_H(p)$ are defined over $\mathbb{Q}\left(\sqrt{p}\right)$ and Galois conjugate. The Manin-Drinfeld theorems tell us that

$$C_H(p)\left(\mathbb{Q}\left(\sqrt{p}\right)\right) \subset J_H(p)\left(\mathbb{Q}\left(\sqrt{p}\right)\right)_{\text{tors}}$$

$J_H(p)\left(\mathbb{Q}\left(\sqrt{p}\right)\right)_{\text{tors}}$

Taking $H = \{a^2 \ : \ a \in (\mathbb{Z}/p\mathbb{Z})^*\}$, where p is prime congruent to 1 modulo 4, the cusps of $X_H(p)$ are defined over $\mathbb{Q}\left(\sqrt{p}\right)$ and Galois conjugate. The Manin-Drinfeld theorems tell us that

$$C_H(p)\left(\mathbb{Q}\left(\sqrt{p}\right)\right) \subset J_H(p)\left(\mathbb{Q}\left(\sqrt{p}\right)\right)_{\text{tors}}$$

and we can ask whether the above is ever an equality.

$J_H(p)\left(\mathbb{Q}\left(\sqrt{p}\right)\right)_{\text{tors}}$

Taking $H = \{a^2 \;:\; a \in (\mathbb{Z}/p\mathbb{Z})^*\}$, where p is prime congruent to 1 modulo 4, the cusps of $X_H(p)$ are defined over $\mathbb{Q}\left(\sqrt{p}\right)$ and Galois conjugate. The Manin-Drinfeld theorems tell us that

$$C_H(p)\left(\mathbb{Q}\left(\sqrt{p}\right)\right) \subset J_H(p)\left(\mathbb{Q}\left(\sqrt{p}\right)\right)_{\text{tors}}$$

and we can ask whether the above is ever an equality.

Theorem

With notation as above, for all p such that the genus of $g = X_H(p)$ is $2 \leq g \leq 10$, we have

$$C_H(p) = J_H(p)\left(\mathbb{Q}\left(\sqrt{p}\right)\right)_{tors}$$

Thank you !