Hyperelliptic and trigonal modular curves in positive charcteristic

Maarten Derickx [1] Filip Najman [2]

[1]Universiteit Leiden

[2]University of Zagreb

Modular curves and Galois representations

Zagreb - 20-09-2023

Slides at: `bit.ly/hyperelliptic-trigonal`

Modular curves

Let $N > 0$ be an integer and $H \subseteq (\mathbb{Z}/N\mathbb{Z})^*$ be a subgroup with $-1 \in H$. Then define:

$$\Gamma_H(N) := \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{PSL}_2(\mathbb{Z}) \,\middle|\, c \in N\mathbb{Z},\ (d \mod N) \in H \right\}$$

$$\Gamma_H(N) \times \overline{\mathbb{H}} \to \overline{\mathbb{H}} : \quad \left(\begin{bmatrix} a & b \\ c & d \end{bmatrix}, z \right) \mapsto \frac{az+b}{cz+d}$$

$$\Gamma_0(N) := \Gamma_{(\mathbb{Z}/N\mathbb{Z})^*}(N), \quad \Gamma_1(N) := \Gamma_{\{\pm 1 \mod N\}}(N)$$

$$X_H(N) := \overline{\mathbb{H}}/\Gamma_H(N)$$

Proposition

The complex curves $X_H(N)$ have a smooth model over $\mathbb{Z}[1/N]$.

Origin story

mathoverflow

Hyperelliptic modular curves in characteristic p

Ask Question

Asked 10 years, 3 months ago Modified 2 months ago Viewed 571 times

7

Ogg characterized the finitely many N such that $X_0(N)_\mathbb{Q}$ is hyperelliptic, and Poonen proved in "Gonality of modular curves in characteristic p" that for large enough N, $X_0(N)_{\mathbb{F}_p}$ is not hyperelliptic.

Question: Are there any N such that $X_0(N)_\mathbb{Q}$ is not hyperelliptic but for some p not dividing N $X_0(N)_{\mathbb{F}_p}$ is hyperelliptic?

I'm also interested in this question for other modular curves of the form X_H, where H is a congruence subgroup.

nt.number-theory ag.algebraic-geometry

Share Cite Edit Follow Flag

asked Jun 3, 2013 at 2:45
David Zureick-Brown

The main Questions

Question

Can one classify the triples $N, p, H \subset (\mathbb{Z}/N\mathbb{Z})^*$ *consisting of an integer, a prime* $p \nmid N$ *and a subgroup such that* $X_H(N)_{\mathbb{F}_p}$ *(or* $X_H(N)_{\overline{\mathbb{F}}_p}$*) is*

- *hyperelliptic,*
- *trigonal, or*
- *of gonality* d *for some integer* d*?*

What about $X_H(N)_{\mathbb{Q}}$ *or* $X_H(N)_{\mathbb{C}}$*?*

Question

Is the set of pairs N, H *for which there exists a prime* p *such that* $X_H(N)_{\overline{\mathbb{F}}_p}$ *is* d*-gonal, finite for every integer* d*?*
Equivalently, can one bound the gonality of $X_H(N)_{\overline{\mathbb{F}}_p}$ *from below in terms of the index* $[\mathrm{PSL}_2(\mathbb{Z}) : \Gamma_H(N)]$ *only?*

Some highlighted results in characteristic 0

Theorem (Ogg (1974))

$X_0(N)$ is hyperelliptic in chracteristic 0 for the following 19 values of N:

$$\{22, 23, 26, 28, 29, 30, 31, 33, 35, 37, 39, 40, 41, 46, 47, 48, 50, 59, 71\}$$

Theorem (Ishii, Momose (1991))

The only other modular curves of the form $X_H(N)$ that are hyperelliptic in characteristic 0 are $X_1(13)$, $X_1(16)$ and $X_1(18)$.

Theorem (Hasegawa, Shimura (1999))

The $\mathbb{C}$-gonality of $X_0(N)$ is 3 $\iff$ $N = 34, 38, 43, 44, 45, 53, 54, 61, 64, 81$.

Theorem (Najman, Orlić (2022))

Classification of the $X_0(N)$ that are of $\mathbb{Q}$-gonality ≤ 6.

Lower bounds

Theorem (Abramovich (1996))

$$\mathrm{gon}(X_H(N)_{\mathbb{Q}}) \geq \mathrm{gon}(X_H(N)_{\mathbb{C}}) \geq \frac{7}{800}[\mathrm{PSL}_2(\mathbb{Z}) : \Gamma_H(N)/(\pm 1)]$$

Theorem (Poonen (2006))

$$\mathrm{gon}(X_H(N)_{\mathbb{F}_{p^2}}) \geq \frac{p-1}{12(p^2+1)}[\mathrm{PSL}_2(\mathbb{Z}) : \Gamma_H(N)/(\pm 1)]$$

$$\mathrm{gon}(X_H(N)_{\overline{\mathbb{F}}_p}) \geq \sqrt{\mathrm{gon}(X_H(N)_{\mathbb{F}_{p^2}})}$$

Question

Does there exist a constant C such that

$$\mathrm{gon}(X_H(N)_K) \geq C[\mathrm{PSL}_2(\mathbb{Z}) : \Gamma_H(N)]$$

for all fields K in which N is invertible?

Castelnuovo-Severi and class numbers

Proposition (Castelnuovo-Severi inequality)

Let $X,\ Y,\ Z$ be nice curves over a perfect field k, with maps $\pi_Y : X \to Y$ and $\pi_Z : X \to Z$ of degrees m and n. Assume that there is no $X \to X'$ of degree > 1 through which both π_Y and π_X factor. Then:

$$g(X) \leq m \cdot g(Y) + n \cdot g(Z) + (m-1)(n-1).$$

Corollary (C-S inequality & Riemann-Hurwitz formula)

Let r_N be the ramifictation degree of $X_0(N) \to X_0(N)^+ := X_0(N)/W_N$. Suppose k is a perfect field in which N is invertible and $f : X_0(N)_k \to \mathbb{P}^1_k$ is a map with $r_N > 2\deg(f)$, then f factors via $X_0(N)^+_k$.

Lemma

$$\text{Suppose } N > 4 \text{ then } r_N = \begin{cases} h(-4N) + h(-N) & \text{if } N \equiv 3 \pmod 4, \\ h(-4N) & \text{otherwise.} \end{cases}$$

Growth of class numbers

Let $D < 0$ be a fundamental discriminant and $f \in \mathbb{N}$. Define $\mathcal{O}_{Df^2}$ as the order of discriminant Df^2 and let $h(Df^2)$ be the classnumber of $_{Df^2}$.

Theorem (Gauss conjecture, Heilbronn (1934))

$h(D) \to \infty$ as $D \to -\infty$

Watkins (2004) classified all fundamental discriminants $D < 0$ such that $h(D) \leq 100$.

Corollary

$r_N \geq h(-4N) > 6$ if $N > 1019$.

Note: There are lots of $N \leq 1019$ such that $r_N > 6$.

The level of hyperelliptic and trigonal modular curves

Corollary

Suppose k is a perfect field s.t. $\mathrm{char}(k) \nmid N$ and $f : X_0(N)_k \to \mathbb{P}^1_k$ is a map with $r_N > 2\deg(f)$, then f factors via $X_0(N)^+_k$.

Proposition (Najman, D.)

Suppose $N > 1019$, k a field s.t. $\mathrm{char}(k) \nmid N$ and $H \subset (\mathbb{Z}/N\mathbb{Z})^*$ a subgroup, then $X_H(N)_k$ is not hyperelliptic and not trigonal.

Proof.

It suffices to restrict to $k = \overline{\mathbb{F}}_p$ with $p \nmid N$. Since gonality can only decrease when taking a quotient of a curve we can also restrict to $H = (\mathbb{Z}/N\mathbb{Z})^*$ and hence $X_H(N) = X_0(N)$. Since $N > 1019$ one has $r_N > 6$, so any $f : X_0(N)_k \to \mathbb{P}^1_k$ of degree ≤ 3 factors via $X_0(N)^+_k$ by the corollary. Since $g(X_0(N)^+_k) > 0$ for $N \geq 73$ this prevents $X_0(N)^+$ from admitting a map of degree ≤ 3 to $\mathbb{P}^1_k$. □

Canonical map

Let X be a nice curve of genus $g > 1$ over a field k.

The canonical ring of X is: $R(X) := \bigoplus_{d=0}^{\infty} H^0(X, \Omega_{X/k}^{\otimes d})$

Let $V := H^0(X, \Omega_{X/k})$ and define $\mathrm{Sym}(V) := \bigoplus_{d=0}^{\infty} \mathrm{Sym}^d(V)$, then the identity map $Sym^1(V) = V \to V = R(X)_1$ induces a natural map of graded rings $f_{can} : \mathrm{Sym}(V) \to R(X)$, and hence we get a map:

$$X \cong \mathrm{Proj}(R(X)) \to \mathrm{Proj}(\mathrm{Sym}(V)) \cong \mathbb{P}_k^{g-1}$$

called the canonical map. The ideal $I_{can} := \ker(f_{can}) \subset \mathrm{Sym}(V)$ is the canonical ideal.

Theorem (Babbage, Chisini, Enrique $\mathrm{char}\, 0$, Saint-Donat $\mathrm{char} > 0$)

X is hyperelliptic $\iff$ the dimension of $I_{can,2} \subseteq Sym^2(V)$ is $\binom{g-1}{2}$.
If X is not hyperelliptic and not a smooth plane quintic then:
X is trigonal over $\overline{k} \iff$ the dimension of $I_{can,3}/(V \cdot I_{can,2})$ is $g - 3$.

Computing the primes of hyperelliptic reduction

Let X be a nice curve of genus $g > 1$ over $\mathbb{Z}[1/N]$, then $V := H^0(X, \Omega_{X/\mathbb{Z}[1/N]})$, $\mathrm{Sym}^2(V)$ and $R(X)_2 := H^0(X, \Omega^{\otimes 2}_{X/\mathbb{Z}[1/N]})$ are free $\mathbb{Z}[1/N]$-modules of rank g, $\binom{g+1}{2}$ and $3g-3$. If $p \nmid N$ one has:

1. $V \otimes \mathbb{F}_p \cong H^0(X_{\mathbb{F}_p}, \Omega_{X/\mathbb{F}_p})$,
2. $\mathrm{Sym}^2(V) \otimes \mathbb{F}_p \cong \mathrm{Sym}^2(V \otimes \mathbb{F}_p)$ and
3. $R(X)_2 \otimes \mathbb{F}_p \cong R(X_{\mathbb{F}_p}) := H^0(X_{\mathbb{F}_p}, \Omega^{\otimes 2}_{X/\mathbb{F}_p})$

$X_{\mathbb{F}_p}$ is hyperelliptic if and only if

$$\dim \ker \left(f_{can,\mathbb{F}_p} : \mathrm{Sym}^2(H^0(X, \Omega_{X/\mathbb{F}_p})) \to H^0(X_{\mathbb{F}_p}, \Omega^{\otimes 2}_{X/\mathbb{F}_p}) \right) = \binom{g-1}{2}$$

The isomorphism 1,2 and 3 above mean we can read off the dimension of this kernel from a smith normal form of the matrix representing

$$\mathrm{Sym}^2(V) \to R(X)_2.$$

One can write down a similar matrix from which you can read off the primes of trigonal reduction.

The main Theorems

Theorem (Najman, D.)

Let $p \nmid N$ then $X_H(N)_{\overline{\mathbb{F}}_p}$ is hyperelliptic if and only if $X_H(N)_{\mathbb{C}}$ is, with exactly one exception.
Namely: if $N = 37$ and $H := \langle 4 \rangle \subset (\mathbb{Z}/37\mathbb{Z})^*$ then $X_H(N)_{\overline{\mathbb{F}}_2}$ is hyperelliptic, but $X_H(N)_{\mathbb{C}}$ as well as $X_H(N)_{\overline{\mathbb{F}}_p}$ with $p > 2$ are trigonal.

Theorem (Najman, D.)

Let $p \nmid N$ then $X_H(N)_{\overline{\mathbb{F}}_p}$ is trigonal if and only if $X_H(N)_{\mathbb{C}}$ is, with exactly one exception.
Namely: $X_0(73)_{\overline{\mathbb{F}}_2}$ is trigonal, however $X_0(73)_{\mathbb{C}}$ as well as $X_0(73)_{\overline{\mathbb{F}}_p}$ with $p > 2$ are tetragonal.

Trigonality over non algebraically closed fields

Proposition (Castelnuovo-Severi inequality)

Let X, Y, Z be nice curves over a perfect field k, with maps $\pi_Y : X \to Y$ and $\pi_Z : X \to Z$ of degrees m and n. Assume that there is no $X \to X'$ of degree > 1 through which both π_Y and π_X factor. Then:

$$g(X) \leq m \cdot g(Y) + n \cdot g(Z) + (m-1)(n-1).$$

Corollary

If $g(X) \geq 5$ and X is trigonal, then the trigonal map is unique.
In particular, if $g(X) \geq 5$ then X_k is trigonal $\iff X_{\overline{k}}$ is trigonal.

Proposition

If $g(X) = 3$ and $X(k) \neq \emptyset$ then X_k is trigonal $\iff X_k$ is not hyperelliptic.
In this case again X_k is trigonal $\iff X_{\overline{k}}$ is trigonal.

Since $X_H(N)(\mathbb{Z}[1/N]) \neq \emptyset$ this means the trigonality over $\mathbb{F}_p$ and $\overline{\mathbb{F}}_p$ can only differ if $g(X_H(N)) = 4$.

Trigonal curves of genus 4

$X_0(N)$ is of genus 4 for $N = 38, 44, 47, 53, 54, 61, 81$.
$X_0(47)$ is hyperelliptic over all fields k with $\operatorname{char} k \nmid N$.
$X_0(54)$ and $X_0(81)$ are trigonal over all fields k with $\operatorname{char} k \nmid N$.
Let $\mathcal{O}_d$ be the quadratic order of discriminant d.

Theorem (Najman, D.)

Let N, d one of the 4 pairs below and k be a field s.t. $\operatorname{char} k \nmid N$ then $X_0(N)_k$ is 3-gonal $\iff$ there exists a morphism $\mathcal{O}_d \to k$.

N	38	44	53	61
d	-3	-8	-15	-4

Proof.

These $X_0(N)$ are the intersection of a quadric of discriminant d and a cubic in $\mathbb{P}^3$. Maps of degree 3 correspond to rulings of the quadric. The rulings are defined over $\mathbb{F}_{p^2}$ if p is inert in $\mathcal{O}_d$, and $\mathbb{F}_p$ otherwise. □

Thank you!

Bonus slide

Theorem (Anni, Assaf, Lorenzo Garcia (2022))

If a modular curve of the form $X_H(N)$ admits a smooth plane model over $\mathbb{C}$, then the degree of this model is at most 18 and not equal to $5, 6$ or 7.

Theorem (Najman, D.)

Let $p \nmid N$ then none of the modular curves $X_H(N)$ admit a smooth plane model of degree 5 over $\overline{\mathbb{F}}_p$.