Gonalities of Modular Curves

Maarten Derickx [1]   Mark van Hoeij [2]

[1] Algant (Leiden, Bordeaux and Milano)

[2] Florida State University

Intercity Number Theory Seminar
01-03-2013

Outline

1. Gonalities
   - Lower bounds
   - Upper bounds
   - Summary

What is known

$$S(d) := \{p \text{ prime} \mid \exists K/\mathbb{Q} \colon [K:\mathbb{Q}] \leq d, \exists E/K \colon E(K)[p] \neq 0\}$$

$$Primes(n) := \{p \text{ prime} \mid p \leq n\}$$

- $S(d)$ is finite (Merel)
- $S(d) \subseteq Primes((3^{d/2}+1)^2)$ (Oesterlé)
- $S(1) = Primes(7)$ (Mazur)
- $S(2) = Primes(13)$ (Kamienny, Kenku, Momose)
- $S(3) = Primes(13)$ (Parent)
- $S(4) = Primes(17)$ (Kamienny, Stein, Stoll) to be published.

New results

$$S(d) := \{p \text{ prime} \mid \exists K/\mathbb{Q} \colon [K:\mathbb{Q}] \le d, \exists E/K \colon E(K)[p] \neq 0\}$$

$$Primes(n) := \{p \text{ prime} \mid p \le n\}$$

- $S(5) = Primes(19)$ (Kamienny, Stein, Stoll and D.)
- $S(6) \subseteq Primes(23) \cup \{37, 73\}$ (Kamienny, Stein, Stoll and D.)

73 is the only prime p for which we do not know whether $p \in S(6)$.

j-invariant

Over $\mathbb{C}$ the j-invariant gives a 1-1 correspondence:

$$j\colon\ \{E/\mathbb{C}\}/_{\sim} \longleftrightarrow \mathbb{C}$$

Now $\mathbb{C} \cong \mathbb{H}/SL_2(\mathbb{Z})$ where $SL_2(\mathbb{Z})$ acts on $\mathbb{H}$ by:

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \tau = \frac{a\tau + b}{c\tau + d}$$

Analytic description: $E = \mathbb{C}/(\tau\mathbb{Z} + \mathbb{Z})$, $q = e^{2\pi i\tau}$

$$j(E) = q^{-1} + 744 + 196884q + 21493760q^2 + \dots$$

Algebraic description: $E = Z(y^2 - x^3 - ax - b)$

$$j(E) = \frac{1728 \cdot 4a^3}{4a^3 + 27b^2}$$

Analytic description of the modular curve $Y_1(N)$

$$\Gamma_1(N) := \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in SL_2(\mathbb{Z}) \mid \begin{bmatrix} a & b \\ c & d \end{bmatrix} \equiv \begin{bmatrix} 1 & * \\ 0 & 1 \end{bmatrix} \mod N \right\}$$

$$Y_1(N)(\mathbb{C}) := \mathbb{H}/\Gamma_1(N)$$

There is again a 1-1 correspondence:

$$\psi : \{(E, P) \mid E/\mathbb{C},\ P \in E \text{ of order } N\}/_\sim \xleftrightarrow{1:1} Y_1(N)(\mathbb{C})$$

Analytic description $(E, P) = (\mathbb{C}/(\tau\mathbb{Z} + \mathbb{Z}), 1/N \mod \tau\mathbb{Z} + \mathbb{Z})$

$$\psi(E, P) = \tau \mod SL_2(\mathbb{Z})$$

Algebraic description of the modular curve $Y_1(N)$

Proposition

Let K be a field, E/K and $P \in E(K)$ of order $N \geq 4$. Then there are unique $b, c \in K$ such that $E \cong Z(Y^2 + cXY + bY - X^3 - bX^2)$ and $P = (0,0)$

- $R := \mathbb{Z}[b, c, \frac{1}{\Delta}]$ with $\Delta := -b^3(16b^2 + (8c^2 - 36c + 27)b + (c-1)c^3)$
- E/R elliptic curve given by $Y^2 + cXY + bY = X^3 + bX^2$
- $P := (0 : 0 : 1)$
- Let $\Phi_N, \Psi_N, \Omega_N \in R$ be s.t. $(\Phi_N\Psi_N : \Omega_N : \Psi_N^3) = NP$

The equation $\Psi_N = 0$ means P has order dividing N. Define F_N by removing form Ψ_N all factors coming from some Ψ_d with $d|N$.

$$Y_1(N)_{\mathbb{Z}[1/N]} := \mathrm{Spec}(R[1/N]/F_N)$$

Algebraic description of the modular curve $Y_1(N)$

- $R := \mathbb{Z}[b, c, \frac{1}{\Delta}]$
- E/R elliptic curve given by $Y^2 + cXY + bY = X^3 + bX^2$
- $P := (0 : 0 : 1)$
- Let $\Phi_N, \Psi_N, \Omega_N \in R$ be s.t. $(\Phi_N \Psi_N : \Omega_N : \Psi_N^3) = NP$

Define F_N by removing form Ψ_N all factors coming from some Ψ_d with $d|N$.

$$Y_1(N)_{\mathbb{Z}[1/N]} := \mathrm{Spec}(R[1/N]/F_N)$$

Let $N \geq 4$ and let K be a field with char$(K) \nmid N$ then

$$\psi : \{(E, P) \mid E/K,\ P \in E(K) \text{ of order } N\}/_\sim \xleftrightarrow{1:1} Y_1(N)(K)$$

Let $(E, P) = (Z(y^2 - cxy - by - x^3 - bx^2), (0, 0))$ then

$$\psi(E, P) = (b, c)$$

Relation between $Y_1(N)$ and $S(d)$

The 1-1 correspondence

$$\psi : \{(E, P) \mid E/K,\ P \in E(K) \text{ of order } N\}/_{\sim} \overset{1:1}{\longleftrightarrow} Y_1(N)(K)$$

gives

$$S(d) := \{p \text{ prime} \mid \exists K/\mathbb{Q} \colon [K : \mathbb{Q}] \leq d,\ \exists E/K \colon E(K)\,[p] \neq 0\} =$$

$$= \{p \text{ prime} \mid \exists K/\mathbb{Q} \colon [K : \mathbb{Q}] \leq d,\ Y_1(p)(K) \neq \emptyset\}$$

So we want to know whether $Y_1(p)$ has any points of degree $\leq d$ over $\mathbb{Q}$.

$X_1(N)$ and cusps

Let $N \geq 5$. Then $Y_1(N)$ can be embedded in a projective $\mathbb{Z}[1/N]$-scheme $X_1(N)$. Let $K = \overline{K}$ and N prime. Then

$$\#(X_1(N)(K) \backslash Y_1(N)(K)) = N - 1.$$

These $N - 1$ elements are called the cusps.
Over $\mathbb{Q}$ we have

$$\#(X_1(N)(\mathbb{Q}) \backslash Y_1(N)(\mathbb{Q})) = (N - 1)/2.$$

i.e. only half of the cusps are defined over $\mathbb{Q}$.

A useful proposition of Michael Stoll

Proposition

Let $C/\mathbb{Q}$ be a smooth proj. geom. irred. curve with Jacobian J, $d \geq 1$ and ℓ a prime of good reduction for C. Let $P \in C(\mathbb{Q})$ and $\iota : C^{(d)} \to J$ the canonical map normalized by $\iota(dP) = 0$. Suppose that:

1. ***there is no non-constant*** $f \in \mathbb{Q}(C)$ ***of degree*** $\leq d$.
2. *$J(\mathbb{Q})$ is finite.*
3. *$\ell > 2$ or $J(\mathbb{Q})[2] \hookrightarrow J(\mathbb{F}_\ell)$.*
4. $C(\mathbb{Q}) \twoheadrightarrow C(\mathbb{F}_\ell)$
5. *The intersection of $\iota(C^{(d)}(\mathbb{F}_\ell)) \subseteq J(\mathbb{F}_\ell)$ with the image of $J(\mathbb{Q})$ under reduction mod ℓ is contained in the image of $C^d(\mathbb{F}_\ell)$.*

Then $C(\mathbb{Q})$ is the set of points of degree $\leq d$ on C.

Definition of gonality

Definition

Let K be a field and C/K be a smooth proj. geom. irred. curve then the K-gonality of C is:

$$\mathrm{gon}_K(C) := \min_{f \in K(C) \setminus K} [K(C) : K(f)] = \min_{f \in K(C) \setminus K} \deg f$$

Theorem (Abramovich)

Let N be a prime then:

$$\mathrm{gon}_{\mathbb{C}}(X_1(N)) \geq \frac{7}{1600}(N^2 - 1).$$

If Selberg's eigenvalue conjecture holds then:

$$\mathrm{gon}_{\mathbb{C}}(X_1(N)) \geq \frac{1}{192}(N^2 - 1).$$

So $\mathrm{gon}_{\mathbb{Q}}(X_1(41)) \geq \mathrm{gon}_{\mathbb{C}}(X_1(41)) \geq 7/1600(41^2 - 1) > 7$.
But, even with the conjecture, this doesn't give a good enough bound for showing $\mathrm{gon}_{\mathbb{Q}}(X_1(29)), \mathrm{gon}_{\mathbb{Q}}(X_1(31)) > 6$

The $\mathbb{F}_\ell$ gonality is smaller than the $\mathbb{Q}$-gonality

Proposition

Let $C/\mathbb{Q}$ be a smooth proj. geom. irred. curve and ℓ be a prime of good reduction of C then:

$$\mathrm{gon}_{\mathbb{Q}}(C) \geq \mathrm{gon}_{\mathbb{F}_\ell}(C_{\mathbb{F}_\ell})$$

To use this we need to know how compute the $\mathbb{F}_\ell$ gonality of C. Let $\mathrm{div}_d^+ C_{\mathbb{F}_\ell} \subseteq \mathrm{div}^+ C_{\mathbb{F}_\ell}$ be the set of effective divisors of degree d. Then $\#(\mathrm{div}_d^+ C_{\mathbb{F}_\ell}) < \infty$. The following algorithm computes the $\mathbb{F}_\ell$-gonality:

Step 1 set $d = 1$

Step 2 While for all $D \in \mathrm{div}_d^+ C_{\mathbb{F}_\ell}$: $\dim H^0(C, D) = 1$ set $d = d + 1$

Step 3 Output d.

This is too slow to compute $\mathrm{gon}_{\mathbb{F}_2}(X_1(29))$ and $\mathrm{gon}_{\mathbb{F}_2}(X_1(31))$

Divisors dominating all functions of degree $\leq d$

$C/\mathbb{F}_l$ a smooth proj. geom. irr. curve. View $f \in \mathbb{F}_l(C)$ as a map $f\colon C \to \mathbb{P}^1_{\mathbb{F}_l}$. For $g \in \operatorname{Aut} C$, $h \in \operatorname{Aut} \mathbb{P}^1_{\mathbb{F}_l}$: $\deg f = \deg h \circ f \circ g$

Definition

A set of divisors $S \subseteq \operatorname{div} C$ dominates all functions of degree $\leq d$ if for all dominant $f\colon C \to \mathbb{P}^1_{\mathbb{F}_l}$ of degree $\leq d$ there are $D \in S$, $g \in \operatorname{Aut} C$ and $h \in \operatorname{Aut} \mathbb{P}^1_{\mathbb{F}_l}$ such that $\operatorname{div} h \circ f \circ g \geq -D$

Proposition

If $S \subseteq \operatorname{div} C$ dominates all functions of degree $\leq d$ then

$$\operatorname{gon}_{\mathbb{F}_l} C \geq \min\Big(d+1, \inf_{\substack{D \in S,\, f \in H^0(C,D), \\ \deg f \neq 0}} \deg f\Big).$$

Example: $\operatorname{div}^+_d C$ dominates all functions of degree $\leq d$.

A smaller set of divisors dominating functions of degree $\leq d$

Proposition

Define $n := \lceil \#C(\mathbb{F}_l)/(l+1) \rceil$ *and* $D := \sum_{p \in C(\mathbb{F}_l)} p$. *Then*

$$\operatorname{div}^+_{d-n} C + D := \left\{ s' + D \mid s' \in \operatorname{div}^+_{d-n} C \right\}$$

dominates all functions of degree $\leq d$.

Proof.

There is a $g \in \operatorname{Aut} \mathbb{P}^1_{\mathbb{F}_l}$ such that $g \circ f$ has poles at at least n distinct points in $C(\mathbb{F}_l)$. If f has degree $\leq d$ then there is an element $s \in \operatorname{div}^+_{d-n} C$ such that $\operatorname{div} g \circ f \geq -s - D$. $\square$

An even smaller set of divisors dominating functions of degree $\leq d$

Proposition

If $S \subseteq \operatorname{div} C$ dominates all functions of degree $\leq d$ and $S' \subseteq \operatorname{div} C$ is such that for all $s \in S$ there are $s' \in S'$ and $g \in \operatorname{Aut} C$ such that $g(s') \geq s$. Then S' also dominates all functions of degree $\leq d$.

This means that only 1 representative of each $\operatorname{Aut} C$ orbit of S is needed. This will be useful in the cases $C = X_1(p)$ with $p = 29, 31$.
In these case we have an automorphism of C for each $d \in (\mathbb{Z}/p\mathbb{Z})^* / \{\pm 1\}$ given by $(E, P) \mapsto (E, dP)$. This gives 14 and 15 automorphisms respectively.

Modular units

Definition

Let K be a field, then an $f \in K(X_1(N))$ K is called a K-rational modular unit if $\operatorname{div} f$ consists entirely of cusps.

Let C be the set of all $Gal(\overline{\mathbb{Q}}/\mathbb{Q})$ orbits of cusps of $X_1(N)$. Let $M \subset \mathbb{Z}^C = (\mathbb{Z}^{cusps})^{Gal(\overline{\mathbb{Q}}/\mathbb{Q})} \subset \mathbb{Z}^{cusps}$ be the set of all principal cuspidal divisors that are rational. Then for each $m \in M$ there is a $\mathbb{Q}$-rational modular unit f such that $m = \operatorname{div} f$.

Idea: If one can compute M then one has a lattice of divisors of functions. Finding short vectors in this lattice will hopefully give good upperbounds on the gonality.

The lattice of modular units using modular symbols

$$\psi : \mathbb{Z}_0^{cusps} \to H_1(X_1(N)(\mathbb{C}), cusps, \mathbb{Z})$$
$$c_1 - c_2 \mapsto \{c_1, c_2\}$$

$$\phi : H_1(X_1(N)(\mathbb{C}), cusps, \mathbb{Z}) \to \frac{\Omega^1(X_1(N)(\mathbb{C}))^\vee}{H_1(X_1(N)(\mathbb{C}), \mathbb{Z})} = J(X_1(N))(\mathbb{C})$$
$$\{c_1, c_2\} \mapsto \left(\omega \mapsto \int_{c_1}^{c_2} \omega\right)$$

im $\phi \subset \frac{H_1(X_1(N))\mathbb{C}),\mathbb{Q})}{H_1(X_1(N)(\mathbb{C}),\mathbb{Z})}$ and furthermore ϕ can be computed entirely using modular symbols. Since $M = (\ker \phi \circ \psi)^{Gal(\overline{\mathbb{Q}}/\mathbb{Q})}$ we can also compute M.

List of computed gonalities

The $\mathbb{Q}$-gonalities of $X_1(N)$ for $N \leq 40$ are:

N	1	2	3	4	5	6	7	8	9	10
gon	1	1	1	1	1	1	1	1	1	1
N	11	12	13	14	15	16	17	18	19	20
gon	2	1	2	2	2	2	4	2	5	3
N	21	22	23	24	25	26	27	28	29	30
gon	4	4	7	4	5	6	6	6	11	6
N	31	32	33	34	35	36	37	38	39	40
gon	12	8	10	10	12	8	18	12	14	12

Let p be the smallest prime s.t. $p \nmid N$. Then $\mathrm{gon}_{\mathbb{Q}} X_1(N) = \mathrm{gon}_{\mathbb{F}_p} X_1(N)$ for the above N.

For all $2 \leq N \leq 40$ there exists a modular unit f with $\deg f = \mathrm{gon}_{\mathbb{Q}} X_1(N)$

The gonalities for $N \leq 22$ and $N = 24$ were already known.