Gonalities of Modular Curves

Maarten Derickx ¹  Mark van Hoeij ²

¹Algant (Leiden, Bordeaux and Milano)
²Florida State University

Intercity Number Theory Seminar
01-03-2013
Outline

1. Gonalities
   - Lower bounds
   - Upper bounds
   - Summary
What is known

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

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

- \(S(d)\) 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

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

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

- \( S(5) = Primes(19) \) (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 \( p \in S(6) \).
**Motivation**

**Modular Curves**

**Gonalities**

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

\[ j: \{ E/\mathbb{C} \}/\sim \leftrightarrow \mathbb{C} \]

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

\[ j(E) = q^{-1} + 744 + 196884q + 21493760q^2 + \ldots \]

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

\[ j(E) = \frac{1728 \cdot 4a^3}{4a^3 + 27b^2} \]
Analytic description of the modular curve $Y_1(N)$

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

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

There is again a 1-1 correspondence:

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

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

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

$E \cong \mathbb{Z}(Y^2 + cXY + bY - X^3 - bX^2)$ 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 $\psi_N$ all factors coming from some $\psi_d$ with $d|N$.

$Y_1(N)_{\mathbb{Z}[1/N]} := \text{Spec}(R[1/N]/F_N)$
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 $\Psi_N$ all factors coming from some $\Psi_d$ with $d | N$.

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

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

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

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

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

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

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

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

These $N - 1$ elements are called the cusps.

Over $\mathbb{Q}$ we have

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

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

Maarten Derickx, Mark van Hoeij

Gonalities of Modular Curves
**Proposition**

Let $C/\mathbb{Q}$ be a smooth proj. geom. irred. curve with Jacobian $J$, $d \geq 1$ and $\ell$ 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 $\ell$ 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 $C$. 

---

Maarten Derickx, Mark van Hoeij  
Gonalities of Modular Curves
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:

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

**Theorem (Abramovich)**

Let $N$ be a prime then:

$$gon_C(X_1(N)) \geq \frac{7}{1600} (N^2 - 1).$$

If Selberg’s eigenvalue conjecture holds then:

$$gon_C(X_1(N)) \geq \frac{1}{192} (N^2 - 1).$$

So $gon_Q(X_1(41)) \geq gon_C(X_1(41)) \geq 7/1600(41^2 - 1) > 7$.

But, even with the conjecture, this doesn’t give a good enough bound for showing $gon_Q(X_1(29)), gon_Q(X_1(31)) > 6$.
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 $\ell$ be a prime of good reduction of $C$ then:

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

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

1. **Step 1** set $d = 1$
2. **Step 2** While for all $D \in \text{div}^+_d C_{\mathbb{F}_\ell} : \dim H^0(C, D) = 1$ set $d = d + 1$
3. **Step 3** Output $d$.

This is too slow to compute $\text{gon}_{\mathbb{F}_2}(X_1(29))$ and $\text{gon}_{\mathbb{F}_2}(X_1(31))$
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 $f : C \to \mathbb{P}^1_{\mathbb{F}_l}$. For $g \in \text{Aut }C$, $h \in \text{Aut }\mathbb{P}^1_{\mathbb{F}_l}$: $\deg f = \deg h \circ f \circ g$

**Definition**

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

**Proposition**

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

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

Example: $\text{div}^+ d C$ dominates all 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

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

dominates all functions of degree $\leq d$.

Proof.

There is a $g \in \text{Aut} \mathbb{P}^1_{\mathbb{F}_l}$ 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 $s \in \text{div}_{d-n}^+ C$ such that $\text{div} g \circ f \geq -s - D$. 

Maarten Derickx, Mark van Hoeij
Gonalities of Modular Curves
An even smaller set of divisors dominating functions of degree $\leq d$

**Proposition**

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

This means that only 1 representative of each $\text{Aut} \ C$ 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 $f \in K(X_1(N))$ is called a $K$-rational modular unit if $\text{div} \; f$ consists entirely of cusps.

Let $C$ be the set of all $\text{Gal}(\overline{Q}/Q)$ orbits of cusps of $X_1(N)$. Let $M \subset \mathbb{Z}^C = (\mathbb{Z}^{\text{cusps}})^{\text{Gal}(\overline{Q}/Q)} \subset \mathbb{Z}^{\text{cusps}}$ 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 $m = \text{div} \; f$.

**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

\[ \psi : \mathbb{Z}_0^{\text{cusps}} \rightarrow H_1(X_1(N)(\mathbb{C}), \text{cusps}, \mathbb{Z}) \]

\[ c_1 - c_2 \mapsto \{c_1, c_2\} \]

\[ \phi : H_1(X_1(N)(\mathbb{C}), \text{cusps}, \mathbb{Z}) \rightarrow \frac{\Omega^1(X_1(N)(\mathbb{C}))^\vee}{H_1(X_1(N)(\mathbb{C}), \mathbb{Z})} = J(X_1(N))(\mathbb{C}) \]

\[ \{c_1, c_2\} \mapsto \left( \omega \mapsto \int_{c_1}^{c_2} \omega \right) \]

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

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

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

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

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

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