Torsion points on elliptic curves and gonalities of modular curves with a focus on gonalities of modular curves.

Maarten Derickx
Mathematisch Instituut
Universiteit Leiden
Graduation talk
25-09-2012
Outline

1. Introduction
2. Modular Curves
3. Gonálities
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 in my thesis

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

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

- \( S(5) \subseteq Primes(19) \cup \{29, 31, 41\} \)
- \( S(6) \subseteq Primes(41) \cup \{73\} \)
- \( S(7) \subseteq Primes(43) \cup \{59, 61, 67, 71, 73, 113, 127\} \)

This is in the "Torsion Points" part of my thesis. Today I will not talk about this, but about how to show \( S(5) = Primes(19) \). This joint work with Michael Stoll and will be published together with the \( S(4) \) result.
Over $\mathbb{C}$ the $j$-invariant gives a 1-1 correspondence:

$$j: \{ E/\mathbb{C}\}/\sim \longleftrightarrow \mathbb{C}$$

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 $E = \mathbb{C}/(\tau \mathbb{Z} + \mathbb{Z})$:

$$j(E) = \tau \mod SL_2(\mathbb{Z})$$

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 $Y_1(N)$

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

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

There is again a 1-1 correspondence:

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

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 $E \cong \mathbb{Z}(Y^2 + cXY + bY - X^3 - bX^2)$ 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 $d|N$.

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

... and gonalities of modular curves.
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 $Y_1(29)$, $Y_1(31)$ and $Y_1(41)$ contain points of degree $\leq 5$ 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 ... and gonality of modular curves.
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 $\ell$ 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. $C(\mathbb{Q}) \to C(\mathbb{F}_\ell)$
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 $C$. 
Mazurs result on $S(1)$ implies that if $p > 7$ then the only rational points on $X_1(p)(\mathbb{Q})$ are the rational cusps.
So if hypotheses $1 – 5$ are satisfied for $X_1(p)$ and $d$ with $p > 7$ and some $\ell$ then $p \notin S(d)$.
Stoll has shown hypotheses $2 – 5$ are satisfied for $\ell = 2$, $d = 5$ and $C = X_1(29)$, $X_1(31)$ or $X_1(41)$.
What remains for proving that $S(5) = Primes(19)$ is:

- For $p = 29, 31$ and $41$ there is no non constant $f \in \mathbb{Q}(X_1(p))$ of degree $\leq 5$.

For $p = 41$ this was already known. For $p = 29, 31$ this is proved in the "gonalities" part of my thesis.
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:

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

**Theorem (Abramovich)**

*Let $N$ be a prime then:*

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

*If Selberg’s eigenvalue conjecture holds then:*

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

So $\text{gon}_\mathbb{Q}(X_1(41)) \geq \text{gon}_C(X_1(41)) \geq 7/1600(41^2 - 1) > 7$.

But, even with the conjecture, this doesn’t give a good enough bound for $\text{gon}_\mathbb{Q}(X_1(29))$ and $\text{gon}_\mathbb{Q}(X_1(31))$. 

... and gonalities of modular curves.
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 $\text{div}^+_d C_{\mathbb{F}_\ell} \subseteq \text{div}^+_\mathbb{F}_\ell$ 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:

**Step 1** set $d = 1$

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

**Step 3** Output $d$.

This is too slow to compute $\text{gon}_{\mathbb{F}_2}(X_1(29))$ and $\text{gon}_{\mathbb{F}_2}(X_1(31))$ and gonalities of modular curves.
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

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

Example: \( \text{div}^+_d C \) 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

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

**dominates all functions of degree $\leq d$.**

**Proof.**

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

Maarten Derickx  ... and gonality 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 Aut $C$ orbit of $S$ is needed. This will be usefull 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.
Computing the $\mathbb{F}_2$-gonality of $X_1(29)$ and $X_1(31)$

**Proposition**

$\text{gon}_{\mathbb{F}_2}(X_1(29)) = 11$ and $\text{gon}_{\mathbb{F}_2}(X_1(31)) = 12$

**Proof.**

For a "smart" choice of $S \subset \text{div} \ X_1(p)$ dominating all function of degree $\leq d$ with $d = 10$ (respectively 11) I computed:

$$\text{gon}_{\mathbb{F}_1}(X_1(p)) \geq \min(d + 1, \inf_{D \in S, f \in H^0(X_1(p), D), \deg f \neq 0} \deg f).$$

using Magma. This gives lower bounds 11 (resp. 12). During this computation I found functions of deg 11 (resp. 12).
Over \( \mathbb{Q} \) there are known functions of degree 11 (respectively 13) on \( X_1(29) \) (respectively \( X_1(31) \)).

**Corollary**

\[
\text{gon}_\mathbb{Q}(X_1(29)) = 11 \text{ and } \text{gon}_\mathbb{Q}(X_1(31)) \in \{12, 13\}
\]

Actually, \( \text{gon}_\mathbb{Q}(X_1(31)) = 12 \) because recently Mark van Hoeij found a function of degree 12 on \( X_1(31) \) defined over \( \mathbb{Q} \).
Summary

- $S(5) = \text{Primes}(19)$ (was $\subseteq \text{Primes}(271)$)
- $S(6) \subseteq \text{Primes}(41) \cup \{73\}$ (was $\subseteq \text{Primes}(773)$)
- $S(7) \subseteq \text{Primes}(127)$ (was $\subseteq \text{Primes}(2281)$)

Work in progress:
Using Michael Stoll’s ideas I am close to proving:

$$\text{Primes}(19) \cup \{37\} \subseteq S(6) \subseteq \text{Primes}(19) \cup \{37, 73\}$$