Gonalities of Modular Curves

Maarten Derickx [1] Mark van Hoeij [2]

[1] Algant (Leiden, Bordeaux and Milano)

[2] Florida State University

17th Workshop on Elliptic Curve Cryptography
16 - 18 Sept. 2013 Leuven

Outline

1. Preliminaries (what are modular curves)
   - Algebraic description of the modular curve $Y_1(N)$
2. Modular Units
3. Gonalities
   - Intro
   - Computing gonalities
   - Motivation

Main idea behind modular curves

Let $N \in \mathbb{N}$ then the set:

$$\left\{ \begin{array}{l} \text{Pairs } (E, P) \text{ of elliptic} \\ \text{curve, point of order} \\ N \end{array} \right\} / \sim$$

has a natural structure of a curve. One can study all pairs (E, P) at the same time by studying the curve C.

$(E_1, P_1) \sim (E_2, P_2)$ if there exists an isomorphism $\phi : E_1 \to E_2$ such that $\phi(P_1) = P_2$.

Example: Multiplication by -1 gives $(E, P) \sim (E, -P)$

Definition (Tate normal form)

Let $b, c \in K$ then $E_{(b,c)}$ is the curve

$$Y^2 + cXY + bY = X^3 + bX^2$$

Remark The discriminant of $E_{(b,c)}$ is:

$$\Delta(b,c) := -b^3(16b^2 + (8c^2 - 36c + 27)b + (c-1)c^3)$$

Proposition

Let E/K an elliptic curve and $P \in E(K)$ of order $N \geq 4$. Then there are unique $b, c \in K$ and an unique isomorphism $\phi : E \to E_{(b,c)}$ such that $\phi(P) = (0,0)$

$$E_{(b,c)} : Y^2 + cXY + bY = X^3 + bX^2$$

Proposition

Let E/K an elliptic curve and $P \in E(K)$ of order ≥ 4. Then there are unique $b, c \in K$ and an unique isomorphism $\phi : E \to E_{(b,c)}$ such that $\phi(P) = (0,0)$

Proof.

- $E : Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6$, $P = (x, y)$
- Translate P to $(0,0)$.
- $E : Y^2 + a_1'XY + a_3'Y = X^3 + a_2'X^2 + a_4'X$, $P = (0,0)$
- Make the tangent line at $(0,0)$ horizontal
- $E : Y^2 + a_1''XY + a_3''Y = X^3 + a_2''X^2$, $P = (0,0)$

$\square$

$$E_{(b,c)} : Y^2 + cXY + bY = X^3 + bX^2$$

Proposition

Let E/K an elliptic curve and $P \in E(K)$ of order ≥ 4. Then there are unique $b, c \in K$ and an unique isomorphism $\phi : E \to E_{(b,c)}$ such that $\phi(P) = (0,0)$

Proof.

- $E : Y^2 + a_1''XY + a_3''Y = X^3 + a_2''X^2,\ P = (0,0)$
- $Y \mapsto u^3 Y,\ X \mapsto u^2 X$ with $u = a_2''/a_3''$
- $E : Y^2 + \frac{a_1'' a_2''}{a_3''}XY + \frac{a_2''^3}{a_3''^2}Y = X^3 + \frac{a_2''^3}{a_3''^2}X^2, P = (0,0)$
- $E = E_{(b,c)}, c = \frac{a_1'' a_2''}{a_3''}, b = \frac{a_2''^3}{a_3''^2}, P = (0,0)$

$\square$

$$E_{(b,c)} : Y^2 + cXY + bY = X^3 + bX^2$$

Proposition

Let E/K an elliptic curve and $P \in E(K)$ of order ≥ 4. Then there are unique $b, c \in K$ and an unique isomorphism $\phi : E \to E_{(b,c)}$ such that $\phi(P) = (0,0)$

$$\left\{ \begin{array}{l} b, c \ \in \ \mathbb{A}^2(K) \ \text{ s.t} \\ \Delta(b,c) \neq 0 \end{array} \right\} \overset{1:1}{\longleftrightarrow} \left\{ \begin{array}{l} \text{Pairs } (E,P) \text{ of elliptic} \\ \text{curve, point of order} \\ \geq 4 \end{array} \right\} / \sim$$

Definition

Let $N \in \mathbb{N}_{\geq 4}$ and char $K \nmid N$ then the modular curve $Y_1(N)_K \subset \mathbb{A}^2_K$ is the curve corresponding to the (E,P) where P has exactly order N.

Definition (Division polynomials for $E_{(b,c)}$ at $P = (0:0:1)$)

Define $\Psi_n, \Phi_n, \Omega_n \in \mathbb{Z}[b,c]$ by:

- $\Psi_1 = 1, \Psi_2 = b, \Psi_3 = b^3, \Psi_4 = b^5(c-1)$
- $\Psi_{m+n}\Psi_{n-m}\Psi_r^2 = \Psi_{n+r}\Psi_{n-r}\Psi_m^2 - \Psi_{m+r}\Psi_{m-r}\Psi_n^2$
- $n = m+1, r = 1 \Rightarrow \Psi_{2m+1} = \Psi_{m+2}\Psi_m^3 - \Psi_{m-1}\Psi_{m+1}^3$
- $n = m+2, r = 1 \Rightarrow b\Psi_{2m+2} = \Psi_{m-1}(\Psi_{m+3}\Psi_m^2 - \Psi_{m+1}\Psi_{m+2}^2)$
- $\Phi_n = -\Psi_{n-1}\Psi_{n+1}\Omega_n = \frac{\Psi_{2n}}{2\Psi_n} - \Psi_n(c\Phi_n + b\Psi_n^2)$

Proposition

Let $N \in \mathbb{Z}$ and view $E_{(b,c)}$ as an elliptic curve over $K(b,c)$ (or $\mathbb{Z}[b,c,\frac{1}{\Delta(b,c)}]$) then

$$N(0:0:1) = (\Phi_N\Psi_N : \Omega_N : \Psi_N^3)$$

$$N(0:0:1) = (\Phi_N \Psi_N : \Omega_N : \Psi_N^3)$$

Proposition

If $(b, c) \in \mathbb{A}^2(K)$, $\Delta(b, c) \neq 0$ *then*

$$N(0:0:1) = (0:1:0) \Leftrightarrow \Psi_N(b, c) = 0$$

Define F_N by removing form Ψ_N all factors coming from some Ψ_d with $d|N$, and all common factors with $\Delta(b, c)$.

Corollary

If char $K \nmid N$ *then* $Y_1(N)_K \subset \mathbb{A}_K^2$ *is given by* $F_N = 0$*,* $\Delta(b, c) \neq 0$*.*

Definition

$X_1(N)_K$ is the projective closure of $Y_1(N)$, i.e. the unique smooth projective curve whose function field is $K(Y_1(N))$. The cusps are $X_1(N)_K \setminus Y_1(N)_K$.

Example $N = 5$

$$\Delta(b, c) = -b^3(16b^2 + (8c^2 - 36c + 27)b + (c - 1)c^3)$$

- $\Psi_5 = (-b + c - 1)b^8$
- $F_5 = -b + c - 1$
- $Y_1(N)$ given by $c = b + 1$, $\Delta(b, c) \neq 0$
- $\Delta(b, b + 1) = -b^5(b^2 + 11b - 1)$
- $X_1(N) \cong \mathbb{P}^1$, cusps are the points given by $b = 0, b = \infty$ and $b^2 + 11b - 1 = 0$, so not all cusps are always defined over K.

Definition

$f \in K(X_1(N))$ is called a modular unit if all its poles and zero's are cusps. Two modular units f, g are called equivalent if $f/g \in K^*$.

Example (N=5)

The cusps of $X_1(5)$ where $b = 0$,$b = \infty$ and $b^2 + 11b - 1 = 0$. Over $\mathbb{Q}$, b and $b^2 + 11b - 1$ form a multiplicative basis for all modular units up to equivalence, over $\mathbb{C}$ one needs $b + (5\sqrt{5} + 11)/2$ as extra generator.

Example

If $N \nmid M$ then $\Psi_M \in K(X_1(N)) = K(b)[c]/F_N$ is a modular unit. Because if $\Psi_M(b, c) = 0$ for $(b, c) \in Y_1(N)(\bar{K})$ then $(0 : 0 : 1) \in E_{(b,c)}(\bar{K})$ has order N and order dividing M.

Definition

$f \in K(X_1(N))$ is called a modular unit if all its poles and zero's are cusps. Two modular units f, g are called equivalent if $f/g \in K^*$.

Conjecture (Hoeij, D.)

$b, \Delta, \Psi_4, \Psi_5, \ldots, \Psi_{\lfloor N/2 \rfloor + 1}$ form a multiplicative basis for the modular units over $\mathbb{Q}$ up to equivalence.

We used a computer to verify the conjecture for $N \leq 100$.

Definition of gonality

Definition

Let K be a field and C/K be a smooth projective curve then the K-gonality of C is:

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

Example (N=5)

$K(X_1(5)) = K(c)[b]/(-b + c - 1) = K(c)$ so $\mathrm{gon}_K(X_1(5)) = 1$

Example

For an elliptic curve E/K one has $\mathrm{gon}_K(E) = 2$.

General bounds

Theorem (Abramovich)

Let N be a prime then:

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

For general N:

$$\mathrm{gon}_{\mathbb{C}}(X_1(N)) \geq \frac{6}{\pi^2}\frac{7}{1600}N^2.$$

Theorem (Poonen)

If char $K = p > 0$ *then* $\mathrm{gon}_K(X_1(N)) \geq \sqrt{\frac{6}{\pi^2}\frac{p-1}{24(p^2+1)}}N$

Proposition

$$\mathrm{gon}_K(X_1(N)) \leq \frac{N^2}{24}$$

Lowerbound for the $\mathbb{Q}$-gonality by computing the $\mathbb{F}_\ell$ gonality

Proposition

Let $C/\mathbb{Q}$ be a smooth projective 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 already becomes to slow for computing $\mathrm{gon}_{\mathbb{F}_2}(X_1(29))$.

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

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

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

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

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 $C = X_1(N)$. In these cases we have an automorphism of C for each $d \in (\mathbb{Z}/N\mathbb{Z})^* / \{\pm 1\}$ given by $(E, P) \mapsto (E, dP)$.

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.

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

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

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

.

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

The 1-1 correspondence

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

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 $\mathbb{Q}$.

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.

Thank you!