A-gonalities of curves and the existence of infinitely many points of degree *d*

Maarten Derickx [1]

[1] Universität Bayreuth

Algorithms in number theory and arithmetic geometry
02-08-2017

Let $M, N, d \in \mathbb{N}$ such that $M \mid N$

Question

Does there exist a number field K with $[K : \mathbb{Q}] = d$ and an elliptic curve E/K such that $E(K)_{tors} \cong \mathbb{Z}/M\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}$?

Definition/Notation

- *$Y_1(M, N)/\mathbb{Z}[1/N]$ is the curve parametrizing triples (E, P, Q) of elliptic curve, with independent points of order M and N.*
- *$X_1(M, N)/\mathbb{Z}[1/N]$ is its projectivisation.*

Question

Does the curve $Y_1(M, N)_{\mathbb{Q}}$ contain a point of degree d over $\mathbb{Q}$?

Question

Does the curve $Y_1(M, N)_{\mathbb{Q}}$ contain ∞ many points of degree d over $\mathbb{Q}$?

Mazur's torsion theorem (d=1)

Theorem (Mazur)

If $E/\mathbb{Q}$ is an elliptic curve then $E(\mathbb{Q})_{tors}$ is isomorphic to one of the following groups:

- $\mathbb{Z}/N\mathbb{Z}$ *for* $1 \leq N \leq 10$ *or* $N = 12$
- $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2N\mathbb{Z}$ *for* $1 \leq N \leq 4$

And each of these groups occurs for infinitely many non isomorphic elliptic curves.

Merel

Definition

A group G is an *elliptic torsion group* of degree d if $G \cong E(K)_{tors}$ for some elliptic curve E/K with $\mathbb{Q} \subseteq K$, $[K : \mathbb{Q}] = d$. The set of all isomorphism classes of such groups is denoted by $\Phi(d)$.

Theorem (Uniform Boundedness Conjecture)

$\Phi(d)$ is finite for all d.

What is known for torsion groups

Definition

Let $\Phi^\infty(d)$ denote the set of $\mathbb{Z}/M\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}$ for which $X_1(M, N)$ has infinitely many places of degree d over $\mathbb{Q}$.

- $\Phi^\infty(d) \subseteq \Phi(d)$
- $\Phi^\infty(1) = \Phi(1) =$ *known* (Mazur)
- $\Phi^\infty(2) = \Phi(2) =$ *known* (Kenku,Momose,Kamienny)
- $\Phi^\infty(3), \Phi^\infty(4) =$ *known* (Jeon,Kim,Park,Schweizer)
- $\Phi^\infty(3) \neq \Phi(3)$ (Najman)
- $\Phi(3) =$ *known* (D.,Etropolski, Hoeij, Morrow, Zureick-Brown)
- The cyclic groups in $\Phi^\infty(d)$ are known for $d \leq 8$ (D., Hoeij)
- $\Phi^\infty(5)$ and $\Phi^\infty(6)$ are known (D., Sutherland)

When has $Y_1(N)$ ∞ many places of degree d

$j \in \mathbb{Q}(X_1(N))$ is a function of degree $[\mathrm{PSL}_2(\mathbb{Z}) : \Gamma_1(N)] \geq \frac{3}{\pi^2} N^2$, hence $Y_1(N)$ has ∞ many places of degree $[\mathrm{PSL}_2(\mathbb{Z}) : \Gamma_1(N)]$.

Theorem (Abramovich)

$$\mathrm{gon}_{\mathbb{C}}(X_1(N)) \geq \frac{7}{800}[\mathrm{PSL}_2(\mathbb{Z}) : \Gamma_1(N)] \qquad (\geq \frac{7}{800}\frac{3}{\pi^2}N^2)$$

Theorem (Frey, (quick corollary of Faltings))

Let K be a number field and C/K be a curve, if C contains ∞ many places of degree d over K then

$$d \geq \mathrm{gon}_K(C)/2$$

Corollary

If $d < \frac{7}{1600}\frac{3}{\pi^2}N^2 \leq \mathrm{gon}_{\mathbb{C}}(X_1(N))/2 \leq \mathrm{gon}_{\mathbb{Q}}(X_1(N))/2$ then $X_1(N)$ contains only finitely many places of deg d.

For $X_1(M, N)$ one has upper and lower bounds quadratic in MN.

Two reasons for the existence of ∞ many places of degree d on a curve X over a number field K

Consider $u : X^{(d)} \to \mathrm{Pic}^d X$ and define $W_d^0(X) := u(X^{(d)})$.

Suppose $X(K) \neq \emptyset$ then one has that $\# X^{(d)}(K)$ is infinite if and only if at least one of the following two condtitions holds.

1) $u(K) : X^{(d)}(K) \to \mathrm{Pic}^d X(K)$ is not injective. In this case there is a fiber of u isomorphic to $\mathbb{P}^r$ with $r > 0$.
2) $\# W_d^0(K) = \infty$. In this case there exists a translate of a positive rank abelian variety $A + x \subseteq W_d^0$ (Faltings).

Remark: If $\# Pic^0 X(K) < \infty$ then $\mathrm{gon}_K X$ is the smallest degree for which X has infinitely many places of degree d over K.

Difficulties in determining $\Phi^\infty(d)$ for $d > 6$

Degree d = 7,8: The (m, mn) for which it is not known if $X_1(m, mn)$ has infinitely many points of degree d all have $\mathrm{rk} J_1(m, mn)(\mathbb{Q}(\zeta_m)) = 0$.
For these (m, mn) it hence suffices to proof $\mathrm{gon}_{\mathbb{Q}}(X_1(m, mn)) > 8$.
The main problem is getting good enough gonality lowerbounds.
Marc-Paul Noordman can do $X_1(2, 2n)$ with n-odd for $d = 7, 8$ using reduction modulo 2, and studying gonalities under bad reduction.

Degree d = 9: a new issue arrises:
The rank of $J_1(37)(\mathbb{Q})$ is 1 and $\mathrm{gon}_{\mathbb{Q}} X_1(37) = 18$.
Need to show that W_9^0 does not contain a translate of $J_0^+(37)$.

Formall immersions and A-gonality

Let X, Y be Noetherian schemes, $\phi : X \to Y$, $x \in X$ and $y = \phi(x)$.

Definition

ϕ is a *formal immersion* at x if $\widehat{\phi^*} : \widehat{\mathcal{O}_{Y,y}} \to \widehat{\mathcal{O}_{X,x}}$ is surjective.

Remark: $\widehat{\phi^*}$ is surjective iff $k(y) \cong k(x)$ and $\mathfrak{m}_y/\mathfrak{m}_y^2 \twoheadrightarrow \mathfrak{m}_x/\mathfrak{m}_x^2$.

Let C be a curve over a field K, $x \in C(K)$, J its Jacobian, $t : J \to A$ a map of Abelian varieties, and $f_{x,d} : C^{(d)} \to J$ given by $D \to \mathcal{O}_C(D - dx)$.

Definition

The A-gonality (or t-gonality) of C is the smallest d such that $t \circ f_{x,d} : C^{(d)} \to A$ is not a formal immersion at some $y \in C^{(d)}(K)$.

Lemma

Define $W_d^0 := f_{x,d}(C^{(d)})$*, if* W_d^0 *contains a translate of* $A' \subseteq \ker t$ *then*

$$\mathrm{gon}_A(C) \le d.$$

J-gonality agrees with the gonality

Let C be a curve over a field K, $x \in C(K)$, and $t : J \to A$. Define:

$$V := t^* H^0(A, \Omega^1_A) \subset H^0(J, \Omega^1_J) = H^0(C, \Omega^1_C).$$

Lemma

Let $D \in C^{(d)}(K)$ then $t \circ f_{x,d}$ is a formal immersion at D if and only if $V \to H^0(C, \Omega^1_C/\Omega^1_C(-D))$ is surjective.

Proposition

$$\text{gon}_J(C) = \text{gon}_K(C)$$

Proof.

If $J = A$ and $t = \text{Id}_J$ then $V = H^0(C, \Omega^1_C)$.
Taking global sections of $\Omega^1_C(-D) \to \Omega^1_C \to \Omega^1_C/\Omega^1_C(-D)$ gives:

$$0 \to H^0(\Omega^1_C(-D)) \to H^0(\Omega^1_C) \to H^0(\Omega^1_C/\Omega^1_C(-D)) \to$$
$$\to H^0(\mathcal{O}_C(D))^\vee \to H^0(\mathcal{O}_C)^\vee \to 0$$

Generalized Hamming weight

Let n be an integer and $n = \sum_{i=0}^{k} \sum_{j=0}^{m_i} b_{i,j}$ be a partition partition of n.

Definition (Generalized Hamming Weight / GHW)

Let $v = (v_{i,j}) \in \mathbb{F}_p^n \cong \bigoplus_{i=0}^{k} \bigoplus_{j=0}^{m_i} \mathbb{F}_p^{b_{i,j}}$, then the GHW of x is

$$h_b(v) = \sum_{i=0}^{k} \sum_{j=0}^{l_i} b_{i,j}$$

where l_i is the largest j for which $v_{i,j} \neq 0$.
l_i is called the multiplicity of v at i.

- Let b_{triv} be the partition with $k = n$ and both m_i and $b_{i,j}$ constant 1.
- $h_{b_{triv}}$ is the classical Hamming weight
- $h_{b_{triv}}(v) \leq h_b(v)$ for all $v \in \mathbb{F}_p^n$ and all partition partitions b.

Generalized Hamming weight and gonalities

Let $C/\mathbb{F}_p$ be a curve and $D = \sum_{i=0}^{k} m_i D_i$ be an effective divisor of degree n and let b_i denote degree of the field of definition of D_i.

Taking the negative parts of the Laurent expansions at the D_i gives a map $H^0(C, \mathcal{O}_C(D)) \to \mathbb{F}_p^n \cong H^0(C, \mathcal{O}_C(D)/\mathcal{O}_C)$.

Write $n = \sum_{i=0}^{k} \sum_{j=0}^{m_i} b_i$.

The degree function on $H^0(C, \mathcal{O}_C(D))$ agrees with the generalized Hamming weight on $\mathbb{F}_p^n$ with respect to the above partition partition. And the GHW multiplicity agrees with the pole multiplicity.

Lemma

Let D be an effective divisor bigger then all effective divisors of degree d, then $\mathrm{gon}(C) = d'$ *for some* $d' \leq d$ *if and only if the image of*

$$H^0(C, \mathcal{O}_C(D)) \to \mathbb{F}_p^n$$

is a generalized geometric linear code with minimum distance d'*.*

Generalized Hamming weight and A-gonalites

Let $C/\mathbb{F}_p$ be a curve, $x \in C(K)$, and $t : J \to A$. Define:

$$V := t^* H^0(A, \Omega^1_A) \subset H^0(J, \Omega^1_J) = H^0(C, \Omega^1_C).$$

Let D be an effecitve divisor of degree n, and define the degree of an $f : H^0(C, \Omega^1/\Omega(-D)) \to \mathbb{F}_p$ to be the degree of the smallest divisor $E \leq D$ such that f factors via $H^0(C, \Omega^1/\Omega(-D)) \to H^0(C, \Omega^1/\Omega(-E))$.

This degree function is a GHW on $\mathbb{F}_p^n \cong H^0(C, \Omega^1/\Omega(-D))^\vee$.

Lemma

Let D be an effective divisor bigger then all effective divisors of degree d, then $\mathrm{gon}_A(C) = d'$ for some $d' \leq d$ if and only if the image of

$$(H^0(C, \Omega^1/\Omega^1(-D))/V)^\vee \to H^0(C, \Omega^1/\Omega^1(-D))^\vee = \mathbb{F}_p^n$$

is a generalized geometric linear code with minimum distance d'.

Remark: The above lemma is even useful for computing $\mathrm{gon}_{\mathbb{F}_p}(C)$ since it avoids the need of computing $H^0(C, \mathcal{O}_C(D))$.

Computing minimum distances

Let n be an integer, $n = \sum_{i=0}^{k} \sum_{j=0}^{m_i} b_{i,j}$ a partition partition of n, and $V \subseteq \bigoplus_{i=0}^{k} \bigoplus_{j=0}^{m_i} \mathbb{F}_p^{b_{i,j}}$ a linear subspace.

Goal: given an interger d decide wether

$$\operatorname{mdist}(V) := \min_{v \in V \setminus \{0\}} h_b(v) \geq d$$

Approach: Enumerate $w_{d'}(v) := \{v \in V | h_b(v) = d'\}$ for all $d \leq d'$.

Define $I = \{(i,j) | 0 \leq i \leq k, 0 \leq j \leq m_i\}$ and given $J \subseteq I$ define $v|_J := (v_x)_{x \in J}$ and $h_I(v) = h_b(v|_J)$.

Naïve enumeration: Define $\operatorname{piv}(V)$ the subset of (i,j)'s such that $\mathbb{F}_p^{b_{i,j}}$ contains pivot column of a basis for V. First enumerate all v such that $h_{\operatorname{piv}(V)}(v) \leq d'$ and return only those with $h_b(v) = d'$.

Remark: Determining $\operatorname{mdist}(V)$ is an NP-complete problem, however sometimes one can do better then Naïve enumeration.

Brouwer-Zimmerman for Generalized Hamming Weights

Main Idea: Suppose we can write $h_b = \sum_{x=0}^{r} h_x$ with $h_x \geq 0$, and let $\sum d_x = d$ be a partition of d.
If $v \in V$, then either $h_b(v) \geq d$ or there is an x such that $h_x(v) < d_x$.
If the enumrations of the $h_x < d_x$ are faster then the naive enumeration of $h_b(v) < d$, then this gives an improvement.

Example

I one writes $\{0 \ldots k\} = \coprod_{x=0}^{r} I_x$ then $h_b = \sum h_{I_x}$. If furthermore the maps $V \to \bigoplus_{i \in I_x} \bigoplus_{j=0}^{m_i} \mathbb{F}_p^{b_{i,j}}$ are injective and $r > 1$, then the enumeration problems $h_{I_x} < d/r$ are often easier then $h_b < d$.

The example can only work if the codimension of $V \subseteq \mathbb{F}_p^n$ is $\geq n/2$.
Enumerating the v with $h_b(v) \leq d$ and $v_{(i,l)} \neq 0$ is easy if $\sum_{j=0}^{l} b_{i,j} \sim d$.
Can use the example after forcing enough of the $v_{(i,j)}$ to be zero.

Example: $X_1(37)$

The image of J_0^+ in $J_1(37)$ is the unique simple sub-abelian variety of rank > 0. The image of J_0^+ is contained in the kernel of

$$t := \langle 2 \rangle - 1 : J_1(37) \to J_1(37).$$

$V := t^* H^0(J_1(37)_{\mathbb{F}_2}, \Omega^1)$ is 38 dimensional, genus of $X_1(37)$ is 40.

Points in $X_1(37)(\overline{\mathbb{F}_2})$

degree	1	2	3	4	5	6	7	8	9
#points/degree	18	0	0	0	0	21	18	0	39

Initial divisor is of degree $765 = 9 \cdot 18 + 6 \cdot 21 + 7 \cdot 18 + 9 \cdot 39$.
Initial code is of dimension $765 - 38 = 727$. Enumeration of the vectors with at least one degree ≥ 6 point in the support is fast.
Code without $d \geq 6$ points is of dimension $9 \cdot 18 - 38 = 124$.
Enumeration of the vectors with at a pole of order ≥ 4 at one of the $\mathbb{F}_2$ points reduces it to a code of dimension $3 \cdot 18 - 38 = 16$.
Can use Brouwer-Zimmerman with 3 partitions to reduce to enumerating vectors of restricted weight $\leq \lfloor 9/3 \rfloor = 3$ in this 16 code.

How I hoped this talk would end:

The image of J_0^+ in $J_1(37)$ is the unique simple sub-abelian variety of rank > 0. The image of J_0^+ is contained in the kernel of

$$t := \langle 2 \rangle - 1 : J_1(37) \to J_1(37).$$

Proposition

One has: $\mathrm{gon}_{t_{\mathbb{Q}}}(X_1(37)_{\mathbb{Q}}) \geq \mathrm{gon}_{t_{\mathbb{F}_2}}(X_1(37)_{\mathbb{F}_2}) > 9$

Theorem

The number of points of degree ≤ 9 over $\mathbb{Q}$ in $X_1(37)(\overline{\mathbb{Q}})$ is finite.

How it actually ends:

The image of $J_0^+(37)$ in $J_1(37)$ is the unique simple sub-abelian variety of rank > 0. The image of $J_0^+(37)$ is contained in the kernel of

$$t := \langle 2 \rangle - 1 : J_1(37) \to J_1(37).$$

Proposition

One has: $\quad \mathrm{gon}_{t_{\mathbb{Q}}}(X_1(37)_{\mathbb{Q}}) \geq \mathrm{gon}_{t_{\mathbb{F}_2}}(X_1(37)_{\mathbb{F}_2}) = 9$

However there is only one $\mathbb{F}_2$ point where the composition

$$X_1(37)^{(d)}_{\mathbb{F}_2} \to J_1(37) \xrightarrow{t} J_1(37)$$

is not a formal immersion while $\# J_0^+(\mathbb{F}_2) = 5$ so one still gets:

Theorem

$W_9^0(X_1(37)_{\mathbb{F}_2})$ *does not contain a translate of* $J_0^+(37)_{\mathbb{F}_2}$.

Corollary

The number of points of degree ≤ 9 *over* $\mathbb{Q}$ *in* $X_1(37)(\overline{\mathbb{Q}})$ *is finite.*