Lightning Talks
June 2, 2020
Session I

2:15 - 2:20	Caleb Springer, Penn State
2:20 - 2:25	Jacob Mayle, University of Illinois at Chicago
2:25 - 2:30	Pip Goodman, University of Bristol
2:30 - 2:35	Jeroen Hanselman, Universität Ulm
2:35 -2:40	Oana Adascalitei, Boston University
2:40 - 2:45	Vishal Arul, MIT
2:45 - 2:50	Emre Sertöz, Leibniz University Hannover

The Structure of the Group of Rational Points of an Abelian Variety over a Finite Field

Caleb Springer
The Pennsylvania State University

June 2, 2020

Background

The Goal

Given an abelian variety A defined over $\mathbb{F}_q$, recognize the group of rational points $A(\mathbb{F}_q)$ as a **module** over the endomorphism ring $\mathrm{End}_{\mathbb{F}_q}(A)$.

- Lenstra solved this problem completely for **elliptic curves**.

Background

The Goal

Given an abelian variety A defined over $\mathbb{F}_q$, recognize the group of rational points $A(\mathbb{F}_q)$ as a **module** over the endomorphism ring $\mathrm{End}_{\mathbb{F}_q}(A)$.

- Lenstra solved this problem completely for **elliptic curves**.
- In the same paper, Lenstra showed that his result does *not* immediately generalize to all **principally polarized ordinary** abelian varieties.

What we still want:

A generalization of Lenstra's theorem that is true, assuming some conditions that are automatic for elliptic curves.

Main Result

Fix $g \geq 1$. Let $A/\mathbb{F}_q$ be simple of dimension g with Frobenius π. Write $R = \mathrm{End}_{\mathbb{F}_q}(A)$, and let Z be the center of R.

(a) If $[\mathbb{Q}(\pi) : \mathbb{Q}] = 2g$ and R is a **Gorenstein ring**, then

$$A(\mathbb{F}_{q^n}) \cong R/R(\pi^n - 1).$$

Main Result

Fix $g \geq 1$. Let $A/\mathbb{F}_q$ be simple of dimension g with Frobenius π. Write $R = \mathrm{End}_{\mathbb{F}_q}(A)$, and let Z be the center of R.

(a) If $[\mathbb{Q}(\pi) : \mathbb{Q}] = 2g$ and R is a **Gorenstein ring**, then

$$A(\mathbb{F}_{q^n}) \cong R/R(\pi^n - 1).$$

(b) If $(\pi^n - 1)Z$ is the product of **invertible prime ideals** in Z, then there is an isomorphism of Z-modules

$$A(\mathbb{F}_{q^n}) \cong (Z/Z(\pi^n - 1))^d.$$

where $d = 2g/[K : \mathbb{Q}]$. The R-module structure comes from an isomorphism of rings

$$R/R(\pi^n - 1) \cong \mathrm{Mat}_d(Z/Z(\pi^n - 1)).$$

Rigidity in Elliptic Curve Local-Global Principles

Jacob Mayle

June 2, 2020

University of Illinois at Chicago

Workshop on Arithmetic Geometry, Number Theory, and Computation

Elliptic curve local-global principles

Let K be a number field, E/K be an elliptic curve, and ℓ be an odd prime.

Elliptic curve local-global principles

Let K be a number field, E/K be an elliptic curve, and ℓ be an odd prime. Define

$$\mathcal{T}_\ell \coloneqq \{\text{primes } \mathfrak{p} \subseteq \mathcal{O}_K : E_\mathfrak{p} \text{ has nontrivial } \mathbb{F}_\mathfrak{p}\text{-rational } \ell\text{-torsion}\},$$

Elliptic curve local-global principles

Let K be a number field, E/K be an elliptic curve, and ℓ be an odd prime. Define

$$\mathcal{T}_\ell \coloneqq \{\text{primes } \mathfrak{p} \subseteq \mathcal{O}_K : E_\mathfrak{p} \text{ has nontrivial } \mathbb{F}_\mathfrak{p}\text{-rational } \ell\text{-torsion}\},$$

$$\mathcal{I}_\ell \coloneqq \{\text{primes } \mathfrak{p} \subseteq \mathcal{O}_K : E_\mathfrak{p} \text{ admits an } \mathbb{F}_\mathfrak{p}\text{-rational } \ell\text{-isogeny}\}.$$

Elliptic curve local-global principles

Let K be a number field, E/K be an elliptic curve, and ℓ be an odd prime. Define

$$\mathcal{T}_\ell \coloneqq \{\text{primes } \mathfrak{p} \subseteq \mathcal{O}_K : E_\mathfrak{p} \text{ has nontrivial } \mathbb{F}_\mathfrak{p}\text{-rational } \ell\text{-torsion}\},$$
$$\mathcal{I}_\ell \coloneqq \{\text{primes } \mathfrak{p} \subseteq \mathcal{O}_K : E_\mathfrak{p} \text{ admits an } \mathbb{F}_\mathfrak{p}\text{-rational } \ell\text{-isogeny}\}.$$

Let $\delta(\mathcal{T}_\ell)$ and $\delta(\mathcal{I}_\ell)$ be the densities of these sets among the prime ideals of $\mathcal{O}_K$.

Elliptic curve local-global principles

Let K be a number field, E/K be an elliptic curve, and ℓ be an odd prime. Define

$$\mathcal{T}_\ell \coloneqq \{\text{primes } \mathfrak{p} \subseteq \mathcal{O}_K : E_\mathfrak{p} \text{ has nontrivial } \mathbb{F}_\mathfrak{p}\text{-rational } \ell\text{-torsion}\},$$
$$\mathcal{I}_\ell \coloneqq \{\text{primes } \mathfrak{p} \subseteq \mathcal{O}_K : E_\mathfrak{p} \text{ admits an } \mathbb{F}_\mathfrak{p}\text{-rational } \ell\text{-isogeny}\}.$$

Let $\delta(\mathcal{T}_\ell)$ and $\delta(\mathcal{I}_\ell)$ be the densities of these sets among the prime ideals of $\mathcal{O}_K$.

Theorem (Katz 1981). If $\delta(\mathcal{T}_\ell) = 1$, then E is K-isogenous to an elliptic curve with nontrivial K-rational ℓ-torsion.

Elliptic curve local-global principles

Let K be a number field, E/K be an elliptic curve, and ℓ be an odd prime. Define

$$\mathcal{T}_\ell \coloneqq \{\text{primes } \mathfrak{p} \subseteq \mathcal{O}_K : E_\mathfrak{p} \text{ has nontrivial } \mathbb{F}_\mathfrak{p}\text{-rational } \ell\text{-torsion}\},$$
$$\mathcal{I}_\ell \coloneqq \{\text{primes } \mathfrak{p} \subseteq \mathcal{O}_K : E_\mathfrak{p} \text{ admits an } \mathbb{F}_\mathfrak{p}\text{-rational } \ell\text{-isogeny}\}.$$

Let $\delta(\mathcal{T}_\ell)$ and $\delta(\mathcal{I}_\ell)$ be the densities of these sets among the prime ideals of $\mathcal{O}_K$.

Theorem (Katz 1981). If $\delta(\mathcal{T}_\ell) = 1$, then E is K-isogenous to an elliptic curve with nontrivial K-rational ℓ-torsion.

Theorem (Sutherland 2012). Suppose $\sqrt{\left(\frac{-1}{\ell}\right)\ell} \notin K$. If $\delta(\mathcal{I}_\ell) = 1$, then E admits an ℓ-isogeny over a quadratic extension of K.

Elliptic curve local-global principles

Let K be a number field, E/K be an elliptic curve, and ℓ be an odd prime. Define

$$\mathcal{T}_\ell := \{\text{primes } \mathfrak{p} \subseteq \mathcal{O}_K : E_\mathfrak{p} \text{ has nontrivial } \mathbb{F}_\mathfrak{p}\text{-rational } \ell\text{-torsion}\},$$
$$\mathcal{I}_\ell := \{\text{primes } \mathfrak{p} \subseteq \mathcal{O}_K : E_\mathfrak{p} \text{ admits an } \mathbb{F}_\mathfrak{p}\text{-rational } \ell\text{-isogeny}\}.$$

Let $\delta(\mathcal{T}_\ell)$ and $\delta(\mathcal{I}_\ell)$ be the densities of these sets among the prime ideals of $\mathcal{O}_K$.

Theorem (Katz 1981). If $\delta(\mathcal{T}_\ell) = 1$, then E is K-isogenous to an elliptic curve with nontrivial K-rational ℓ-torsion.

Theorem (Sutherland 2012). Suppose $\sqrt{\left(\frac{-1}{\ell}\right)\ell} \notin K$. If $\delta(\mathcal{I}_\ell) = 1$, then E admits an ℓ-isogeny over a quadratic extension of K.

Question. If $\delta(\mathcal{T}_\ell) \neq 1$, then how large may $\delta(\mathcal{T}_\ell)$ be? Similarly for $\delta(\mathcal{I}_\ell)$.

Rigidity of the locally everywhere conditions

Let $G(\ell) \subseteq \mathrm{GL}_2(\mathbb{F}_\ell)$ denote the image of the mod ℓ Galois representation of E.

Rigidity of the locally everywhere conditions

Let $G(\ell) \subseteq \mathrm{GL}_2(\mathbb{F}_\ell)$ denote the image of the mod ℓ Galois representation of E.

It follows from properties of $G(\ell)$ and the Chebotarev density theorem that

Rigidity of the locally everywhere conditions

Let $G(\ell) \subseteq \mathrm{GL}_2(\mathbb{F}_\ell)$ denote the image of the mod ℓ Galois representation of E.

It follows from properties of $G(\ell)$ and the Chebotarev density theorem that

1. $\delta(\mathcal{T}_\ell)$ is the proportion of matrices in $G(\ell)$ with 1 as an eigenvalue,

Rigidity of the locally everywhere conditions

Let $G(\ell) \subseteq \mathrm{GL}_2(\mathbb{F}_\ell)$ denote the image of the mod ℓ Galois representation of E.

It follows from properties of $G(\ell)$ and the Chebotarev density theorem that

1. $\delta(\mathcal{T}_\ell)$ is the proportion of matrices in $G(\ell)$ with 1 as an eigenvalue,
2. $\delta(\mathcal{I}_\ell)$ is the proportion of matrices in $G(\ell)$ with some eigenvalue in $\mathbb{F}_\ell$.

Rigidity of the locally everywhere conditions

Let $G(\ell) \subseteq \mathrm{GL}_2(\mathbb{F}_\ell)$ denote the image of the mod ℓ Galois representation of E.

It follows from properties of $G(\ell)$ and the Chebotarev density theorem that

1. $\delta(\mathcal{T}_\ell)$ is the proportion of matrices in $G(\ell)$ with 1 as an eigenvalue,
2. $\delta(\mathcal{I}_\ell)$ is the proportion of matrices in $G(\ell)$ with some eigenvalue in $\mathbb{F}_\ell$.

Considering subgroups of $\mathrm{GL}_2(\ell)$ case-by-case along Dickson's theorem, we prove:

Rigidity of the locally everywhere conditions

Let $G(\ell) \subseteq \mathrm{GL}_2(\mathbb{F}_\ell)$ denote the image of the mod ℓ Galois representation of E.

It follows from properties of $G(\ell)$ and the Chebotarev density theorem that

1. $\delta(\mathcal{T}_\ell)$ is the proportion of matrices in $G(\ell)$ with 1 as an eigenvalue,
2. $\delta(\mathcal{I}_\ell)$ is the proportion of matrices in $G(\ell)$ with some eigenvalue in $\mathbb{F}_\ell$.

Considering subgroups of $\mathrm{GL}_2(\ell)$ case-by-case along Dickson's theorem, we prove:

Theorem (M. 2020). $\delta(\mathcal{T}_\ell), \delta(\mathcal{I}_\ell) \notin (\frac{3}{4}, 1)$.

Rigidity of the locally everywhere conditions

Let $G(\ell) \subseteq \mathrm{GL}_2(\mathbb{F}_\ell)$ denote the image of the mod ℓ Galois representation of E.

It follows from properties of $G(\ell)$ and the Chebotarev density theorem that

1. $\delta(\mathcal{T}_\ell)$ is the proportion of matrices in $G(\ell)$ with 1 as an eigenvalue,
2. $\delta(\mathcal{I}_\ell)$ is the proportion of matrices in $G(\ell)$ with some eigenvalue in $\mathbb{F}_\ell$.

Considering subgroups of $\mathrm{GL}_2(\ell)$ case-by-case along Dickson's theorem, we prove:

Theorem (M. 2020). $\delta(\mathcal{T}_\ell), \delta(\mathcal{I}_\ell) \notin (\frac{3}{4}, 1)$.

This rigidity differentiates the local-global principles of Katz & Sutherland with, for instance, the Hasse-Minkowski theorem where failures are quite limited.

References

- S. Anni, *A local–global principle for isogenies of prime degree over number fields*, J. Lond. Math. Soc. (2) **89** (2014), no. 3, 745–761.
- N.M. Katz, *Galois properties of torsion points on abelian varieties*, Invent. Math. **62** (1981), no. 3, 481–502.
- J. Mayle, *Rigidity in elliptic curve local-global principles*, arXiv:2005.05881 (2020).
- A.V. Sutherland, *A local-global principle for rational isogenies of prime degree*, J. Théor. Nombres Bordeaux **24** (2012), no. 2, 475–485.
- I. Vogt, *A local-global principle for isogenies of composite degree*, arXiv:1801.05355 (2018).

Thank you!

Superelliptic curves with large Galois images

Pip Goodman

University of Bristol

2nd June 2020

Notation

- r a prime
- $f \in \mathbb{Q}[x]$ a polynomial without repeated roots
- C superelliptic curve associated to the smooth affine model $y^r = f(x)$
- J the jacobian of C

Theorem (G.'20)

Suppose $2r|d$ can be written as the sum of two primes $q_1 < q_2$ and there exists a prime $q_2 + 2 < q_3 < d$.
Then we may construct an explicit polynomial $f \in \mathbb{Q}[x]$ of degree d such that for all primes l outside of a finite explicit set the image of the representation

$$\rho_l : G_{\mathbb{Q}} \to \mathrm{Aut}(J[l])$$

is as large as possible.

Notation

- r a prime
- $f \in \mathbb{Q}[x]$ a polynomial without repeated roots
- C superelliptic curve associated to the smooth affine model $y^r = f(x)$
- J the jacobian of C

Theorem (G.'20)

Suppose $2r|d$ can be written as the sum of two primes $q_1 < q_2$ and there exists a prime $q_2 + 2 < q_3 < d$.
Then we may construct an explicit polynomial $f \in \mathbb{Q}[x]$ of degree d such that for all primes l outside of a finite explicit set the image of the representation

$$\rho_l : G_{\mathbb{Q}} \to \mathrm{Aut}(J[l])$$

is as large as possible.

Outline/what's different

- Restrict to
$$\rho_l : G_{\mathbb{Q}(\zeta_{rl})} \to \mathrm{Aut}(J[l]).$$
- The image of ρ_l on this subgroup then lands in the centraliser of $[\zeta_r]$ in $\mathrm{Sp}_{2g}(l)$.
- Let t be the number of primes above l in $\mathbb{Q}(\zeta_r)$. If i the inertia degree of a prime above l in $\mathbb{Q}(\zeta_r)$ is odd, then
$$C_{\mathrm{Sp}_{2g}(l)}(\zeta_r) \cong \mathrm{GL}_{a_1}(l^i) \times \cdots \times \mathrm{GL}_{a_{t/2}}(l^i),$$
otherwise
$$C_{\mathrm{Sp}_{2g}(l)}(\zeta_r) \cong \mathrm{GU}_{a_1}(l^{i/2}) \times \cdots \times \mathrm{GU}_{a_t}(l^{i/2}),$$
where $a_j = a_k$ for any j, k.
- Classify maximal subgroups of $\mathrm{GL}_n(l^i)$ and $\mathrm{GU}_n(l^{i/2})$ containing a "generalised transvection".
- Unlike almost all other Galois image papers, we **do not use/need transvections**.
- Control of inertia groups away from l using T. Dokchitser's "Models of curves over DVRs".
- New method for primitivity which **does not require restrictions** on the ground field.

Outline/what's different

- Restrict to
$$\rho_l : G_{\mathbb{Q}(\zeta_{rl})} \to \mathrm{Aut}(J[l]).$$
- The image of ρ_l on this subgroup then lands in the centraliser of $[\zeta_r]$ in $\mathrm{Sp}_{2g}(l)$.
- Let t be the number of primes above l in $\mathbb{Q}(\zeta_r)$. If i the inertia degree of a prime above l in $\mathbb{Q}(\zeta_r)$ is odd, then
$$C_{\mathrm{Sp}_{2g}(l)}(\zeta_r) \cong \mathrm{GL}_{a_1}(l^i) \times \cdots \times \mathrm{GL}_{a_{t/2}}(l^i),$$
otherwise
$$C_{\mathrm{Sp}_{2g}(l)}(\zeta_r) \cong \mathrm{GU}_{a_1}(l^{i/2}) \times \cdots \times \mathrm{GU}_{a_t}(l^{i/2}),$$
where $a_j = a_k$ for any j, k.
- Classify maximal subgroups of $\mathrm{GL}_n(l^i)$ and $\mathrm{GU}_n(l^{i/2})$ containing a "generalised transvection".
- Unlike almost all other Galois image papers, we **do not use/need transvections**.
- Control of inertia groups away from l using T. Dokchitser's "Models of curves over DVRs".
- New method for primitivity which **does not require restrictions** on the ground field.

Outline/what's different

- Restrict to
$$\rho_l : G_{\mathbb{Q}(\zeta_{rl})} \to \mathrm{Aut}(J[l]).$$
- The image of ρ_l on this subgroup then lands in the centraliser of $[\zeta_r]$ in $\mathrm{Sp}_{2g}(l)$.
- Let t be the number of primes above l in $\mathbb{Q}(\zeta_r)$. If i the inertia degree of a prime above l in $\mathbb{Q}(\zeta_r)$ is odd, then
$$C_{\mathrm{Sp}_{2g}(l)}(\zeta_r) \cong \mathrm{GL}_{a_1}(l^i) \times \cdots \times \mathrm{GL}_{a_{t/2}}(l^i),$$
otherwise
$$C_{\mathrm{Sp}_{2g}(l)}(\zeta_r) \cong \mathrm{GU}_{a_1}(l^{i/2}) \times \cdots \times \mathrm{GU}_{a_t}(l^{i/2}),$$
where $a_j = a_k$ for any j, k.
- Classify maximal subgroups of $\mathrm{GL}_n(l^i)$ and $\mathrm{GU}_n(l^{i/2})$ containing a "generalised transvection".
- Unlike almost all other Galois image papers, we **do not use/need transvections**.
- Control of inertia groups away from l using T. Dokchitser's "Models of curves over DVRs".
- New method for primitivity which **does not require restrictions** on the ground field.

Outline/what's different

- Restrict to
$$\rho_l : G_{\mathbb{Q}(\zeta_{rl})} \to \mathrm{Aut}(J[l]).$$
- The image of ρ_l on this subgroup then lands in the centraliser of $[\zeta_r]$ in $\mathrm{Sp}_{2g}(l)$.
- Let t be the number of primes above l in $\mathbb{Q}(\zeta_r)$. If i the inertia degree of a prime above l in $\mathbb{Q}(\zeta_r)$ is odd, then
$$C_{\mathrm{Sp}_{2g}(l)}(\zeta_r) \cong \mathrm{GL}_{a_1}(l^i) \times \cdots \times \mathrm{GL}_{a_{t/2}}(l^i),$$
otherwise
$$C_{\mathrm{Sp}_{2g}(l)}(\zeta_r) \cong \mathrm{GU}_{a_1}(l^{i/2}) \times \cdots \times \mathrm{GU}_{a_t}(l^{i/2}),$$
where $a_j = a_k$ for any j, k.
- Classify maximal subgroups of $\mathrm{GL}_n(l^i)$ and $\mathrm{GU}_n(l^{i/2})$ containing a "generalised transvection".
- Unlike almost all other Galois image papers, we **do not use/need transvections**.
- Control of inertia groups away from l using T. Dokchitser's "Models of curves over DVRs".
- New method for primitivity which **does not require restrictions** on the ground field.

The endomorphism character

- $E = \mathrm{End}_K^0(A)$ acts on $V_l(A)$. Thus $V_l(A)$ is an $E \otimes \mathbb{Q}_l$-module.
- The decomposition $E \otimes \mathbb{Q}_l \cong \prod_{\lambda|l} E_\lambda$ induces $V_l \cong \prod_{\lambda|l} V_\lambda$.
- The action of E commutes with of G_K, giving representations

$$\rho_\lambda : G_K \to \mathrm{Aut}_{E_\lambda}(V_\lambda).$$

- The $(\det \circ \rho_\lambda)_\lambda$ form a strictly compatible system of abelian λ-adic representations.
- By work of Ribet they arise from an algebraic Hecke Character Ω, which we call **the endomorphism character** of A with respect to E.

Theorem (G.'20)

Let $\mathfrak{p}$ be a prime of good reduction for $J/\mathbb{Q}(\zeta_r)$ with residual degree one. Suppose $Z\left(\mathrm{End}^0(J_\mathfrak{p})\right)$ is a field and $\mathbb{Q}(\zeta_r) \hookrightarrow Z\left(\mathrm{End}^0(J_\mathfrak{p})\right)$. Then the infinity type of Ω is described by the Newton polygon of C.

- One may often find such a prime by computation.
- Costa, Lombardo and Voight have shown such a primes exists if the Mumford-Tate conjecture holds for $J/\mathbb{Q}(\zeta_r)$.
- If $2r|\deg(f)$, the Mumford-Tate conjecture for $J/\mathbb{Q}(\zeta_r)$ holds by work of Vasiu.

The endomorphism character

- $E = \mathrm{End}_K^0(A)$ acts on $V_l(A)$. Thus $V_l(A)$ is an $E \otimes \mathbb{Q}_l$-module.
- The decomposition $E \otimes \mathbb{Q}_l \cong \prod_{\lambda|l} E_\lambda$ induces $V_l \cong \prod_{\lambda|l} V_\lambda$.
- The action of E commutes with of G_K, giving representations

$$\rho_\lambda : G_K \to \mathrm{Aut}_{E_\lambda}(V_\lambda).$$

- The $(\det \circ \rho_\lambda)_\lambda$ form a strictly compatible system of abelian λ-adic representations.
- By work of Ribet they arise from an algebraic Hecke Character Ω, which we call **the endomorphism character** of A with respect to E.

Theorem (G.'20)

Let $\mathfrak{p}$ be a prime of good reduction for $J/\mathbb{Q}(\zeta_r)$ with residual degree one. Suppose $Z\left(\mathrm{End}^0(J_\mathfrak{p})\right)$ is a field and $\mathbb{Q}(\zeta_r) \hookrightarrow Z\left(\mathrm{End}^0(J_\mathfrak{p})\right)$. Then the infinity type of Ω is described by the Newton polygon of C.

- One may often find such a prime by computation.
- Costa, Lombardo and Voight have shown such a primes exists if the Mumford-Tate conjecture holds for $J/\mathbb{Q}(\zeta_r)$.
- If $2r|\deg(f)$, the Mumford-Tate conjecture for $J/\mathbb{Q}(\zeta_r)$ holds by work of Vasiu.

The endomorphism character

- $E = \mathrm{End}_K^0(A)$ acts on $V_l(A)$. Thus $V_l(A)$ is an $E \otimes \mathbb{Q}_l$-module.
- The decomposition $E \otimes \mathbb{Q}_l \cong \prod_{\lambda|l} E_\lambda$ induces $V_l \cong \prod_{\lambda|l} V_\lambda$.
- The action of E commutes with of G_K, giving representations

$$\rho_\lambda : G_K \to \mathrm{Aut}_{E_\lambda}(V_\lambda).$$

- The $(\det \circ \rho_\lambda)_\lambda$ form a strictly compatible system of abelian λ-adic representations.
- By work of Ribet they arise from an algebraic Hecke Character Ω, which we call **the endomorphism character** of A with respect to E.

Theorem (G.'20)

Let $\mathfrak{p}$ be a prime of good reduction for $J/\mathbb{Q}(\zeta_r)$ with residual degree one. Suppose $Z\left(\mathrm{End}^0(J_\mathfrak{p})\right)$ is a field and $\mathbb{Q}(\zeta_r) \hookrightarrow Z\left(\mathrm{End}^0(J_\mathfrak{p})\right)$. Then the infinity type of Ω is described by the Newton polygon of C.

- One may often find such a prime by computation.
- Costa, Lombardo and Voight have shown such a primes exists if the Mumford-Tate conjecture holds for $J/\mathbb{Q}(\zeta_r)$.
- If $2r|\deg(f)$, the Mumford-Tate conjecture for $J/\mathbb{Q}(\zeta_r)$ holds by work of Vasiu.

The endomorphism character

- $E = \mathrm{End}_K^0(A)$ acts on $V_l(A)$. Thus $V_l(A)$ is an $E \otimes \mathbb{Q}_l$-module.
- The decomposition $E \otimes \mathbb{Q}_l \cong \prod_{\lambda|l} E_\lambda$ induces $V_l \cong \prod_{\lambda|l} V_\lambda$.
- The action of E commutes with of G_K, giving representations

$$\rho_\lambda : G_K \to \mathrm{Aut}_{E_\lambda}(V_\lambda).$$

- The $(\det \circ \rho_\lambda)_\lambda$ form a strictly compatible system of abelian λ-adic representations.
- By work of Ribet they arise from an algebraic Hecke Character Ω, which we call **the endomorphism character** of A with respect to E.

Theorem (G.'20)

Let $\mathfrak{p}$ be a prime of good reduction for $J/\mathbb{Q}(\zeta_r)$ with residual degree one. Suppose $Z\left(\mathrm{End}^0(J_\mathfrak{p})\right)$ is a field and $\mathbb{Q}(\zeta_r) \hookrightarrow Z\left(\mathrm{End}^0(J_\mathfrak{p})\right)$. Then the infinity type of Ω is described by the Newton polygon of C.

- One may often find such a prime by computation.
- Costa, Lombardo and Voight have shown such a primes exists if the Mumford-Tate conjecture holds for $J/\mathbb{Q}(\zeta_r)$.
- If $2r|\deg(f)$, the Mumford-Tate conjecture for $J/\mathbb{Q}(\zeta_r)$ holds by work of Vasiu.

Gluing curves along their 2-torsion

Let X, Y be (nice) curves of genus 1 and genus 2 over a base field k.

Goal:

Find a curve Z (if it exists) over k such that there is an isogeny:

$$\phi : \mathrm{Jac}(X) \times \mathrm{Jac}(Y) \to \mathrm{Jac}(Z)$$

with $\ker\phi \subset (\mathrm{Jac}(X) \times \mathrm{Jac}(Y))\,[2]$.

Results

- Explicit description of gluing data, which gives: Necessary conditions for when a gluing exists over k.
- Analytic Algorithm $\Rightarrow$ Construct period matrix of $\mathrm{Jac}(Z)$ and reconstruct curve using algorithm by Lercier, Ritzenthaler,Sijsling.
- Formula using interpolation that uses X, Y and gluing data as input.

Results

- Geometric Algorithm

$$\begin{array}{ccc} Z = X \times_{\mathrm{Kum}(Y)} \mathrm{Jac}(Y) & \dashrightarrow & \mathrm{Jac}(Y) \\ \downarrow \overline{\pi} & & \downarrow \pi \\ X & \dashrightarrow & \mathrm{Kum}(Y) \end{array} .$$

- Reverses construction by Ritzenthaler, Romagny.

Above methods described in (H., Schiavone, Sijsling)

Rational Points of Fermat Quartics

Oana Adascalitei

Boston University

June 2, 2020

Introduction

In the 1990s J.-P. Serre challenged the mathematical community to find all the rational points of the Fermat quartic which has the affine model

$$\mathcal{F} : x^4 + y^4 = 17.$$

Are there any other solutions beyond

$$\{(\pm 2, \pm 1), (\pm 1, \pm 2)\}?$$

Would any classical method work?

- Chabauty-Coleman: $\mathrm{genus}(\mathcal{F}) = 3$, $\mathrm{rank}(\mathrm{Jac}(\mathcal{F})) = 6$.
- Manin-Demjanenko:

$$\mathrm{Jac}(\mathcal{F}) \sim E_1 \times E_1 \times E_2,$$

where $\mathrm{rank}(E_1) = \mathrm{rank}(E_2) = 2$.

Flynn-Wetherell

In early 2000s, V. Flynn and J. Wetherell developed techniques to address this challenging problem. Their strategy employed a cover for their original curve, which they combined with the elliptic Chabauty method.

Theorem (Flynn, Wetherell)

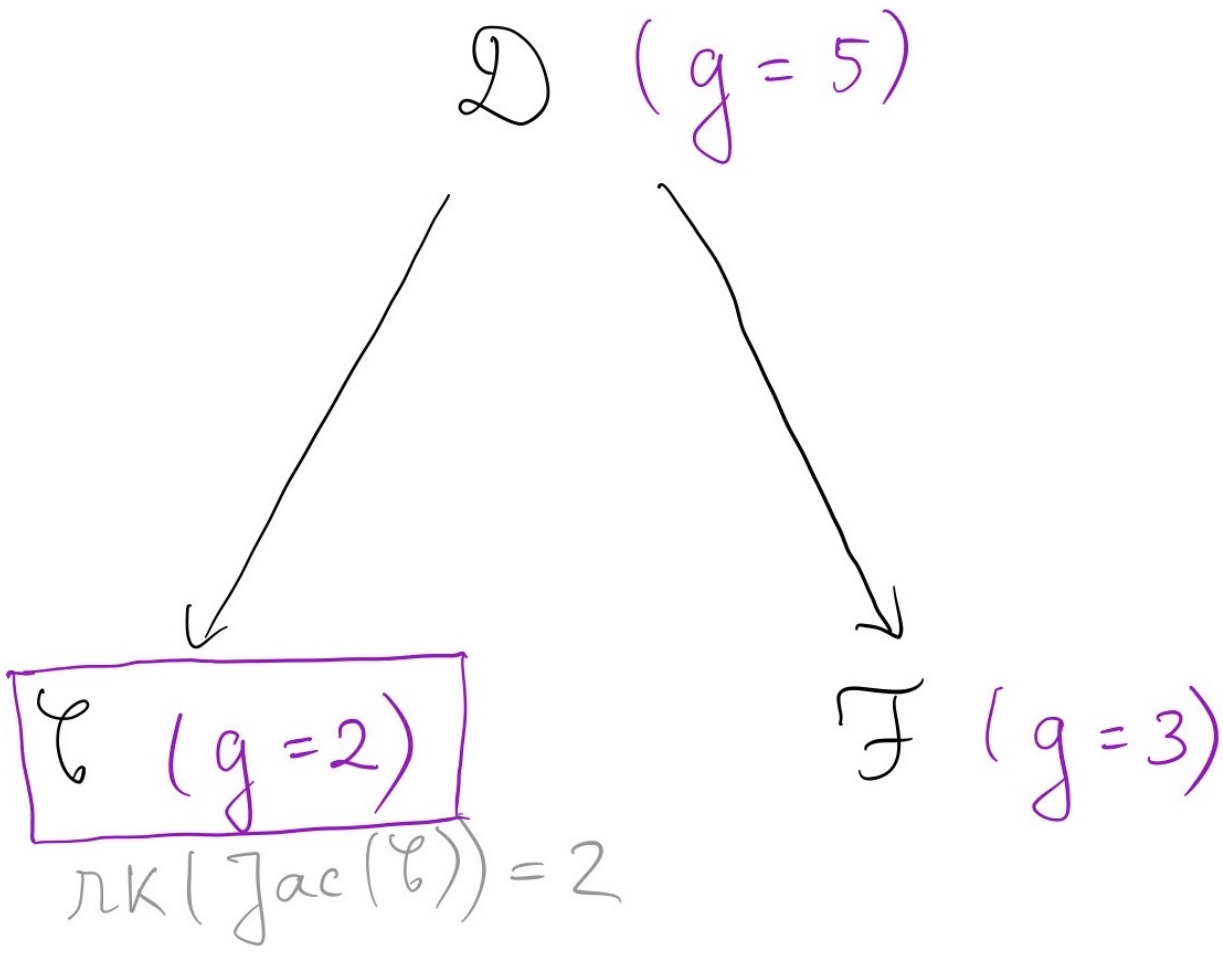
The Fermat quartic

$$x^4 + y^4 = 17$$

has exactly 8 *rational solutions:*

$$\{(\pm 1, \pm 2), (\pm 2, \pm 1)\}.$$

Covering Technique



Understanding the genus 2 curve

- We write the curve in the affine form

$$\boxed{\mathcal{C} : y^2 = F(x) = (9x^2 - 28x + 18)(x^2 + 12x + 2)(x^2 - 2)}.$$

- Proving that $\mathcal{F}(\mathbb{Q}) = \{(\pm 2, \pm 1), (\pm 1, \pm 2)\}$ boils down to showing that $\boxed{\mathcal{C}(\mathbb{Q}) = \{\infty^+, \infty^-\}}$.
- The rest of the proof relies heavily on the fact that $D_1 = [\infty^+ - \infty^-]$ and D_2 are two independent points of infinite order on $\mathrm{Jac}(\mathcal{C})$, where D_2 has Mumford representation $(5x^2 - 18x + 17, 3(-603x + 1187)/50)$.

What about $x^4 + y^4 = 97$?

A natural question to ask after dealing with the $c = 17$ case is whether the same techniques can be employed to solve other values of c which produce the same type of Jacobian. From the point of view of ranks, $c = 17, 97, 257$ look the same, and all of them can be written in the form $c = a^4 + b^4$, with $a, b \in \mathbb{Z}$.

What about $x^4 + y^4 = 97$?

- When we try to replicate the proof from $c = 17$, we again get a genus 2 curve whose Jacobian has rank 2, namely:

$$\mathcal{C} : y^2 = f(x) = (25x^2 - 76x + 50)(x^2 + 28x + 2)(x^2 - 2).$$

- We again would like to find two linearly independent infinite order points on the Jacobian.
- We can again make use of $[\infty^+ - \infty^-]$, but a search in a box could not yield a second point, making us notice that an increase in the value of c may make the cover $\mathcal{C}$ less tractable.

Finding a Point of Infinite Order via Richelot Isogenies

- $J(\mathcal{C}) \sim J(E_1) \times J(E_2)$, given by $\psi_1 : \mathcal{C} \to E_1$ and $\psi_2 : \mathcal{C} \to E_2$
- The elliptic curve E_1 is defined over the quadratic field $L = \mathbb{Q}(\sqrt{97})$ and $E_1(L)$ has rank 2. With the help of Magma, we are able to find two independent points of infinite order in $E_1(L)$.
- Taking the preimage of a point in $E_1(L)$ under the covering map ψ_1 we get a point on $\mathcal{C}$ defined over a quartic extension of $\mathbb{Q}$. Using two such points we can construct a point on $J(\mathcal{C})$ defined over a quadratic extension, and then with two such conjugate points we can construct a point in $J(\mathcal{C})(\mathbb{Q})$.

Conclusion

The Fermat quartic

$$x^4 + y^4 = 97$$

has exactly 8 rational solutions:

$$\{(\pm 3, \pm 2), (\pm 2, \pm 3)\}.$$

Thank you for your attention!

Explicit arithmetic of superelliptic curves and jacobians

Vishal Arul

MIT

June 2, 2020

A superelliptic curve is the smooth projective model of $y^n = f(x)$ over a field K such that $\mathrm{char}(K) \nmid n$, $f(x) \in K[x]$ is separable, and $(n, \deg f) = 1$. A superelliptic curve with $n = 2$ is an odd-degree hyperelliptic curve.

Let $\mathcal{C}$ be a superelliptic curve of genus g and let $\mathcal{J}$ be its jacobian. The automorphism $\zeta\colon (x, y) \mapsto (x, \zeta_n y)$ of $\mathcal{C}$ induces an automorphism ζ of $\mathcal{J}$.

I did the following in my thesis.

1. I provided a formula for "division by $1 - \zeta$" for points of $\mathcal{C}$. Given a point P of $\mathcal{C}$, I write down formulas for every effective degree g divisor such that $[(1 - \zeta)D] = [P - \infty]$. When $n = 2$, this is the same as division by 2, and reduces to Zarhin's formulas for division by 2 on odd-degree hyperelliptic curves. As an application, one can divide points of the form $(\alpha, 0)$ on P to describe all elements of $\mathcal{J}[(1 - \zeta)^2]$. When $n = 3$, $\mathcal{J}[(1 - \zeta)^2] = \mathcal{J}[3]$, so we can write down all the 3-torsion of the jacobian.

2. The roots of the L-polynomial of the "superelliptic Catalan curve" $y^p = x^q + 1$ are Jacobi sums $J(\chi_p, \chi_q)$ where χ_p and χ_q are characters of order p and q. I found new congruences for such Jacobi sums and use these congruences to give an explicit description of the fields of definition of $\mathcal{J}[p]$ and $\mathcal{J}[q]$.
3. A torsion point of $\mathcal{C}$ is a geometric point P of $\mathcal{C}$ such that $[P - \infty]$ has finite order in $\mathcal{J}$. I classified torsion points on $y^n = x^d + 1$ when $n, d, g \geq 2$ and $(n, d) = 1$, generalizing earlier work of Grant-Shaulis, who considered the case when $n = 2$ and d is prime. Any point with $x = 0$ or $y = 0$ is automatically a torsion point; call a torsion point *exceptional* if $x \neq 0$ and $y \neq 0$. I show that the exceptional cases only occur when $n + d = 7$, and I determine all exceptional torsion points in these cases.

Separating periods of quartic surfaces

Emre Can Sertöz

joint with Pierre Lairez (Inria)

Leibniz Universität Hannover

June 02, 2020

Periods to algebraic cycles

Periods $=\{$ Integrals of algebraic functions over algebraic domains$\}$

$$\pi = 2\int_{-1}^{1} \sqrt{1-x^2}\,\mathrm{d}x$$

$a, b \in$ Periods, $a = b \iff \exists$ an algebraic cycle in a variety over $\overline{\mathbb{Q}}$

$X = Z(f) \subset \mathbb{P}^3$, $f \in \mathbb{Z}[x,y,z,w]_4$, $\omega_f \in \mathrm{H}^{2,0}(X/\mathbb{Q})$

$$\text{Periods of } X = \left\{ \int_\gamma \omega_f \;\middle|\; \gamma \in \mathrm{H}_2(X,\mathbb{Z}) \right\}.$$

Lefschetz (1,1)-theorem: $\int_\gamma \omega_f = 0 \iff \gamma = [C_1] - [C_2]$

An analogy with algebraic numbers

$\alpha \in \overline{\mathbb{Q}}$:	(min poly., approx.)	degree, height
$\int_\gamma \omega_f$:	(f, γ)	Δ_γ, $\lvert f \rvert$.

There is an effective constant $\varepsilon(\Delta_\gamma, f)$ such that:

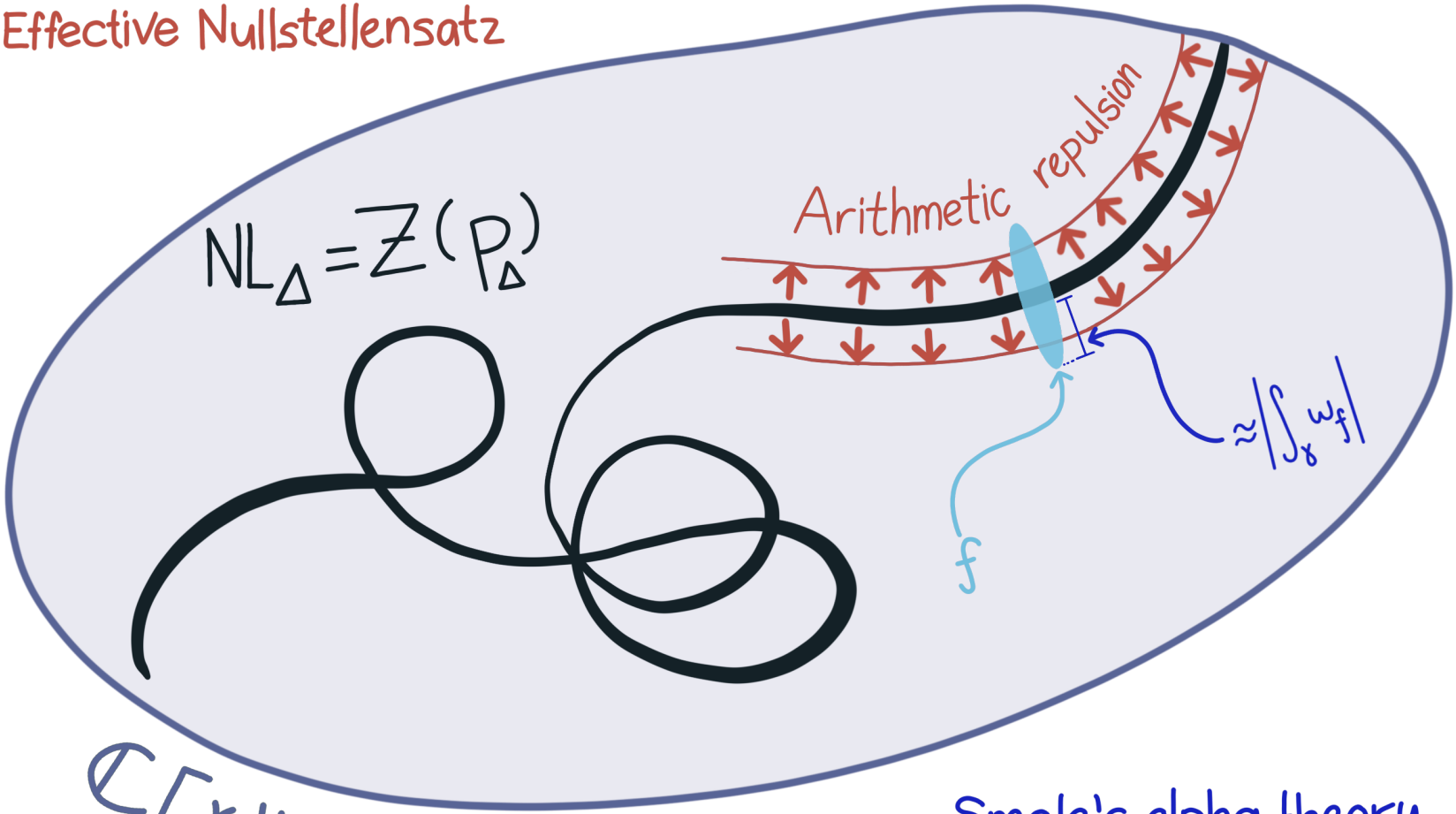
$$\int_\gamma \omega_f = 0 \quad \text{or} \quad \left| \int_\gamma \omega_f \right| > \varepsilon(\Delta_\gamma, f).$$

$$\varepsilon(\Delta, f) = \frac{\left(d_\Delta! |p_\Delta| \left(1 + |f|\right)^{d_\Delta} \right)^{-1}}{4 \| \mathrm{d}\mathcal{P}_f^{-1} \| \left(1 + 6 \frac{\|A\|}{\mathrm{vol}(X_f)} \right)}$$

$\sum_{n \geq 0} \left(2 \uparrow\uparrow (3^n)\right)^{-1}$ is not a ratio of periods of a quartic surface/$\mathbb{Q}$.

Idea

Hilbert schemes
Effective Nullstellensatz



$\mathbb{C}[x,y,z,w]_4 \cong \mathbb{C}^{35}$

Smale's alpha theory
Griffiths–Dwork reduction