Local torsion of elliptic curves

Jędrzej Garnek

Adam Mickiewicz University, Poznan

Torsion groups and Galois representations of elliptic curves
25.06.2018

Local torsion problem

Conjecture (folklore)

Suppose that $E/\mathbb{Q}$ is an elliptic curve without CM. Then for almost all primes p:

$$E(\mathbb{Q}_p)[p] = 0.$$

p-DEGREE CONJECTURE

Definition

p-degree of an elliptic curve $E/\mathbb{Q}$:

$$d_p(E) = \min\{[L : \mathbb{Q}_p] : E(L)[p] \neq 0\}$$

p-degree conjecture

Definition

p-degree of an elliptic curve $E/\mathbb{Q}$:

$$d_p(E) = \min\{[L : \mathbb{Q}_p] : E(L)[p] \neq 0\}$$

A more general conjecture:

Conjecture (David & Weston, 2008)

If $E/\mathbb{Q}$ is an elliptic curve and $\operatorname{End} E = \mathbb{Z}$, *then:*

$$\lim_{p \to \infty} d_p(E) = \infty.$$

p-DEGREE CONJECTURE

Definition

p-degree of an elliptic curve $E/\mathbb{Q}$:

$$d_p(E) = \min\{[L : \mathbb{Q}_p] : E(L)[p] \neq 0\}$$

A more general conjecture:

Conjecture (David & Weston, 2008)

If $E/\mathbb{Q}$ is an elliptic curve and $\operatorname{End} E = \mathbb{Z}$, *then:*

$$\lim_{p \to \infty} d_p(E) = \infty.$$

Motivation: the deformation theory of Galois representations.

What happens for elliptic curves with CM?

p-degree of elliptic curves with CM

What happens for elliptic curves with CM?

Theorem (J.G., 2018)

Let $E : y^2 = x^3 - x$. Then for any prime $p \neq 2, 3$:

$$d_p(E) =$$

p-DEGREE OF ELLIPTIC CURVES WITH CM

What happens for elliptic curves with CM?

Theorem (J.G., 2018)

Let $E : y^2 = x^3 - x$. Then for any prime $p \neq 2, 3$:

$$d_p(E) = \begin{cases} p^2 - 1, & \text{for } p \equiv 3 \pmod 4, \\ & \end{cases}$$

p-degree of elliptic curves with CM

What happens for elliptic curves with CM?

Theorem (J.G., 2018)

Let $E : y^2 = x^3 - x$. Then for any prime $p \neq 2, 3$:

$$d_p(E) = \begin{cases} p^2 - 1, & \text{for } p \equiv 3 \pmod 4, \\ \mathrm{ord}_p(2s), & \text{for } p \equiv 1 \pmod 4, \end{cases}$$

p-degree of elliptic curves with CM

What happens for elliptic curves with CM?

Theorem (J.G., 2018)

Let $E : y^2 = x^3 - x$. Then for any prime $p \neq 2, 3$:

$$d_p(E) = \begin{cases} p^2 - 1, & \text{for } p \equiv 3 \pmod 4, \\ \operatorname{ord}_p(2s), & \text{for } p \equiv 1 \pmod 4, \end{cases}$$

where s is defined for $p \equiv 1 \pmod 4$ by $p = s^2 + t^2$

p-degree of elliptic curves with CM

What happens for elliptic curves with CM?

Theorem (J.G., 2018)

Let $E : y^2 = x^3 - x$. Then for any prime $p \neq 2, 3$:

$$d_p(E) = \begin{cases} p^2 - 1, & \text{for } p \equiv 3 \pmod 4, \\ \operatorname{ord}_p(2s), & \text{for } p \equiv 1 \pmod 4, \end{cases}$$

where s is defined for $p \equiv 1 \pmod 4$ by $p = s^2 + t^2$ and

$$2 \nmid s, \qquad s + t \equiv 1 \pmod 4.$$

p-degree of elliptic curves with CM

What happens for elliptic curves with CM?

Theorem (J.G., 2018)

Let $E : y^2 = x^3 - x$. Then for any prime $p \neq 2, 3$:

$$d_p(E) = \begin{cases} p^2 - 1, & \text{for } p \equiv 3 \pmod 4, \\ \operatorname{ord}_p(2s), & \text{for } p \equiv 1 \pmod 4, \end{cases}$$

where s is defined for $p \equiv 1 \pmod 4$ by $p = s^2 + t^2$ and

$$2 \nmid s, \qquad s + t \equiv 1 \pmod 4.$$

Original proof: main theorem of complex multiplication.

p-DEGREE OF ELLIPTIC CURVES WITH CM

COROLLARY (J.G., 2018)

For

$$E : y^2 = x^3 - x$$

p-DEGREE OF ELLIPTIC CURVES WITH CM

Corollary (J.G., 2018)

For

$$E : y^2 = x^3 - x$$

we have

$$d_p(E) = 8$$

p-degree of elliptic curves with CM

Corollary (J.G., 2018)

For

$$E : y^2 = x^3 - x$$

we have

$$d_p(E) = 8$$

if and only if p is of the form $s_{k+1}^2 + s_k^2$, where:

COROLLARY (J.G., 2018)

For

$$E : y^2 = x^3 - x$$

we have

$$d_p(E) = 8$$

if and only if p is of the form $s_{k+1}^2 + s_k^2$, where:

$$s_0 = 0, \quad s_1 = 1, \quad s_{k+2} = 4s_{k+1} - s_k.$$

p-DEGREE OF ELLIPTIC CURVES WITH CM

COROLLARY (J.G., 2018)

For

$$E : y^2 = x^3 - x$$

we have

$$d_p(E) = 8$$

if and only if p is of the form $s_{k+1}^2 + s_k^2$, where:

$$s_0 = 0, \quad s_1 = 1, \quad s_{k+2} = 4s_{k+1} - s_k.$$

REMARK

$(s_{k+1}^2 + s_k^2)_{k=1}^{100\,000}$ is a prime iff

$$k \in \{1, 2, 3, 4, 5, 131, 200, 296, 350, 519, 704, 950, 5598,$$

$$6683, 7445, 8775, 8786, 11565, 12483\}.$$

$$d_p(E) = \begin{cases} p^2 - 1, & \text{for } p \equiv 3 \pmod 4, \\ \mathrm{ord}_p(2s), & \text{for } p \equiv 1 \pmod 4, \end{cases}$$

$$(\text{for } E : y^2 = x^3 - x)$$

Both parts of the formula

$$d_p(E) = \begin{cases} p^2 - 1, & \text{for } p \equiv 3 \pmod 4, \\ \operatorname{ord}_p(2s), & \text{for } p \equiv 1 \pmod 4, \end{cases}$$

$$(\text{for } E : y^2 = x^3 - x)$$

may be generalized!

p-DEGREE OF SUPERSINGULAR ELLIPTIC CURVES

Theorem (J.G., 2018)

If $E/\mathbb{Q}_p$ has good supersingular reduction then

$$d_p(E) = p^2 - 1.$$

Proof: study of the formal group law of $E \Rightarrow$ for any $P \in E[p]$:

$$e(\mathbb{Q}_p(P)/\mathbb{Q}_p) = p^2 - 1.$$

p-degree of supersingular elliptic curves

Theorem (J.G., 2018)

If $E/\mathbb{Q}_p$ has good supersingular reduction then

$$d_p(E) = p^2 - 1.$$

Proof: study of the formal group law of $E \Rightarrow$ for any $P \in E[p]$:

$$e(\mathbb{Q}_p(P)/\mathbb{Q}_p) = p^2 - 1.$$

By Elkies' results:

Corollary

For any elliptic curve $E/\mathbb{Q}$:

$$\limsup_{p \to \infty} d_p(E) = \infty.$$

Canonical lifts

Definition

Canonical lift of an ordinary elliptic curve $E/\mathbb{F}_q$:

$$\text{the only lift } \mathbb{E}/W(\mathbb{F}_q) \text{ of } E \text{ with CM.}$$

Canonical lifts

Definition

Canonical lift of an ordinary elliptic curve $E/\mathbb{F}_q$:

$$\text{the only lift } \mathbb{E}/W(\mathbb{F}_q) \text{ of } E \text{ with CM.}$$

Theorem (Gross; David & Weston; Garnek)

The following conditions are „almost equivalent":

Canonical lifts

Definition

Canonical lift of an ordinary elliptic curve $E/\mathbb{F}_q$:

$$\text{the only lift } \mathbb{E}/W(\mathbb{F}_q) \text{ of } E \text{ with CM.}$$

Theorem (Gross; David & Weston; Garnek)

The following conditions are „almost equivalent":

(1) $d_p(E) < p - 1$,

Canonical lifts

Definition

Canonical lift of an ordinary elliptic curve $E/\mathbb{F}_q$:

the only lift $\mathbb{E}/W(\mathbb{F}_q)$ of E with CM.

Theorem (Gross; David & Weston; Garnek)

The following conditions are „almost equivalent":

(1) $d_p(E) < p - 1$,

(2) $E_{\mathbb{F}_p}$ *is ordinary and* $E_{\mathbb{Z}/p^2}$ *is a canonical lift of* $E_{\mathbb{F}_p}$,

Canonical lifts

Definition

Canonical lift of an ordinary elliptic curve $E/\mathbb{F}_q$:

$$\text{the only lift } \mathbb{E}/W(\mathbb{F}_q) \text{ of } E \text{ with CM.}$$

Theorem (Gross; David & Weston; Garnek)

The following conditions are „almost equivalent”:

(1) $d_p(E) < p - 1$,

(2) $E_{\mathbb{F}_p}$ *is ordinary and* $E_{\mathbb{Z}/p^2}$ *is a canonical lift of* $E_{\mathbb{F}_p}$,

(3) $E(\mathbb{Q}_p^{un})[p] \neq 0$,

Canonical lifts

Definition

Canonical lift of an ordinary elliptic curve $E/\mathbb{F}_q$:

$$\text{the only lift } \mathbb{E}/W(\mathbb{F}_q) \text{ of } E \text{ with CM.}$$

Theorem (Gross; David & Weston; Garnek)

The following conditions are „almost equivalent":

(1) $d_p(E) < p - 1$,

(2) $E_{\mathbb{F}_p}$ *is ordinary and* $E_{\mathbb{Z}/p^2}$ *is a canonical lift of* $E_{\mathbb{F}_p}$,

(3) $E(\mathbb{Q}_p^{un})[p] \neq 0$,

(4) $E_{\mathbb{F}_p}$ *is ordinary and* $d_p(E) = \operatorname{ord}_p a_p(E)$.

Canonical lifts

Definition

Canonical lift of an ordinary elliptic curve $E/\mathbb{F}_q$:

the only lift $\mathbb{E}/W(\mathbb{F}_q)$ of E with CM.

Theorem (Gross; David & Weston; Garnek)

The following conditions are „almost equivalent":

(1) $d_p(E) < p - 1$,

(2) $E_{\mathbb{F}_p}$ *is ordinary and* $E_{\mathbb{Z}/p^2}$ *is a canonical lift of* $E_{\mathbb{F}_p}$,

(3) $E(\mathbb{Q}_p^{un})[p] \neq 0$,

(4) $E_{\mathbb{F}_p}$ *is ordinary and* $d_p(E) = \operatorname{ord}_p a_p(E)$.

Precisely, "almost equivalent" =

$$(1) \Rightarrow (2), \quad (2) \Leftrightarrow (3), \quad (3) \Rightarrow (4).$$

Open problems

Question

What is the behaviour of $d_p(E)$ for $p \to \infty$ for other elliptic curves $E/\mathbb{Q}$?

Open problems

Question

What is the behaviour of $d_p(E)$ for $p \to \infty$ for other elliptic curves $E/\mathbb{Q}$?

Question

How often is an elliptic curve $E/\mathbb{Q}$ the canonical lift $\bmod p^2$ of its reduction $\bmod p$?

Open problems

Question

What is the behaviour of $d_p(E)$ for $p \to \infty$ for other elliptic curves $E/\mathbb{Q}$?

Question

How often is an elliptic curve $E/\mathbb{Q}$ the canonical lift $\bmod p^2$ of its reduction $\bmod p$?

What about abelian varieties?

Open problems

Question

What is the behaviour of $d_p(E)$ for $p \to \infty$ for other elliptic curves $E/\mathbb{Q}$?

Question

How often is an elliptic curve $E/\mathbb{Q}$ the canonical lift $\bmod p^2$ of its reduction $\bmod p$?

What about abelian varieties?

Question

Fix a Jacobian $A/\mathbb{Q}$. How often is the canonical lift of $A \bmod p$ a Jacobian $\bmod p^2$?

Class numbers of abelian varieties

As a by-product...

Class numbers of abelian varieties

As a by-product...

- $A/\mathbb{Q}$ – an abelian variety of dimension d,
- r – rank of $A(\mathbb{Q})$ over $\mathrm{End}_{\mathbb{Q}}(A)$,
- p – a fixed prime number,
- $K_n := \mathbb{Q}(A[p^n])$ – p^nth division field of A

Class numbers of abelian varieties

As a by-product...

- $A/\mathbb{Q}$ – an abelian variety of dimension d,
- r – rank of $A(\mathbb{Q})$ over $\mathrm{End}_{\mathbb{Q}}(A)$,
- p – a fixed prime number,
- $K_n := \mathbb{Q}(A[p^n])$ – p^nth division field of A

Question

How to estimate the class number of K_n?

Theorem (J.G., 2018)

If either of the following conditions holds:

- $r > d$,
- $r \geqslant 1$, A *has good reduction at* p *and* $A_{\mathbb{F}_p}[p] \neq 0$,

then for some explicit $C = C(A, p) > 0$, $D = D(A, p) > 0$*:*

$$\# \mathrm{Cl}(K_n) \geqslant p^{Cn-D}.$$

Theorem (J.G., 2018)

If either of the following conditions holds:

- $r > d$,
- $r \geqslant 1$, A *has good reduction at* p *and* $A_{\mathbb{F}_p}[p] \neq 0$,

then for some explicit $C = C(A, p) > 0$, $D = D(A, p) > 0$*:*

$$\# \mathrm{Cl}(K_n) \geqslant p^{Cn-D}.$$

Idea of the proof:

Theorem (J.G., 2018)

If either of the following conditions holds:

- $r > d$,
- $r \geqslant 1$, A *has good reduction at* p *and* $A_{\mathbb{F}_p}[p] \neq 0$,

then for some explicit $C = C(A, p) > 0$, $D = D(A, p) > 0$*:*

$$\# \mathrm{Cl}(K_n) \geqslant p^{Cn-D}.$$

Idea of the proof:

- investigate the Kummer extension of $\mathbb{Q}(A[p^n])$,

Theorem (J.G., 2018)

If either of the following conditions holds:

- $r > d$,
- $r \geqslant 1$, *A has good reduction at p and* $A_{\mathbb{F}_p}[p] \neq 0$,

then for some explicit $C = C(A, p) > 0$, $D = D(A, p) > 0$*:*

$$\# \mathrm{Cl}(K_n) \geqslant p^{Cn-D}.$$

Idea of the proof:

- investigate the Kummer extension of $\mathbb{Q}(A[p^n])$,
- switch to local extension to give a bound on inertia groups.

Bibliography:

J. Garnek.
On p-degree of elliptic curves
International Journal of Number Theory, 2018.

J. Garnek.
On the class numbers of division fields of abelian varieties
(preprint)

Thank you for your attention!