Kummer Theory for Elliptic Curves

Sebastiano Tronto

Luxembourg/Leiden

2019-11-29

Classic Kummer Theory

Let K be a number field; let $a \in K^\times$ not a root of unity.

Classic Kummer Theory

Let K be a number field; let $a \in K^\times$ not a root of unity.

- Consider the splitting field L of $X^N - a$

Classic Kummer Theory

Let K be a number field; let $a \in K^\times$ not a root of unity.

- Consider the splitting field L of $X^N - a$
- L contains the N-th cyclotomic extension $K(\zeta_N)$

Classic Kummer Theory

Let K be a number field; let $a \in K^\times$ not a root of unity.

- Consider the splitting field L of $X^N - a$
- L contains the N-th cyclotomic extension $K(\zeta_N)$
- $L \mid K$ and $L \mid K(\zeta_N)$ are Galois

Classic Kummer Theory

Let K be a number field; let $a \in K^\times$ not a root of unity.

- Consider the splitting field L of $X^N - a$
- L contains the N-th cyclotomic extension $K(\zeta_N)$
- $L \mid K$ and $L \mid K(\zeta_N)$ are Galois
- These extensions can be studied explicitly

Kummer Theory - Computing Degrees

The degree $[L : K(\zeta_N)]$ is very close to N.

Kummer Theory - Computing Degrees

The degree $[L : K(\zeta_N)]$ is very close to N.
For explicit computations:

The degree $[L : K(\zeta_N)]$ is very close to N.
For explicit computations:

- Properties of $K(\zeta_N) \mid K$ (does K intersect $\mathbb{Q}(\zeta_N)$?)

Kummer Theory - Computing Degrees

The degree $[L : K(\zeta_N)]$ is very close to N.
For explicit computations:

- Properties of $K(\zeta_N) \mid K$ (does K intersect $\mathbb{Q}(\zeta_N)$?)
- Properties of a (is it an N-th power?)

Kummer Theory - Computing Degrees

The degree $[L : K(\zeta_N)]$ is very close to N.
For explicit computations:

- Properties of $K(\zeta_N) \mid K$ (does K intersect $\mathbb{Q}(\zeta_N)$?)
- Properties of a (is it an N-th power?)
- Relations between $\sqrt[N]{a}$ and ζ_M

Kummer Theory - Computing Degrees

The degree $[L : K(\zeta_N)]$ is very close to N.
For explicit computations:

- Properties of $K(\zeta_N) \mid K$ (does K intersect $\mathbb{Q}(\zeta_N)$?)
- Properties of a (is it an N-th power?)
- Relations between $\sqrt[N]{a}$ and ζ_M

If $K = \mathbb{Q}$ an efficient implementation exists (no splitting field computation required).

E elliptic curve over a number field K.

E elliptic curve over a number field K.
$P \in E(K)$ not torsion ($NP \neq 0$ for every $N \geq 1$).

E elliptic curve over a number field K.
$P \in E(K)$ not torsion ($NP \neq 0$ for every $N \geq 1$).

- There are N^2 points $Q_1, \dots, Q_{N^2} \in E(\overline{K})$ such that $NQ_i = P$ (notation: $N^{-1}P := \{Q_1, \dots, Q_{N^2}\}$)

E elliptic curve over a number field K.
$P \in E(K)$ not torsion ($NP \neq 0$ for every $N \geq 1$).

- There are N^2 points $Q_1, \dots, Q_{N^2} \in E(\overline{K})$ such that $NQ_i = P$ (notation: $N^{-1}P := \{Q_1, \dots, Q_{N^2}\}$)
- Consider $L = K(N^{-1}P)$

Kummer Theory for Elliptic Curves

E elliptic curve over a number field K.
$P \in E(K)$ not torsion ($NP \neq 0$ for every $N \geq 1$).

- There are N^2 points $Q_1, \ldots, Q_{N^2} \in E(\overline{K})$ such that $NQ_i = P$ (notation: $N^{-1}P := \{Q_1, \ldots, Q_{N^2}\}$)
- Consider $L = K(N^{-1}P)$
- L contains the N-th torsion field $K(E[N])$

E elliptic curve over a number field K.
$P \in E(K)$ not torsion ($NP \neq 0$ for every $N \geq 1$).

- There are N^2 points $Q_1, \ldots, Q_{N^2} \in E(\overline{K})$ such that $NQ_i = P$ (notation: $N^{-1}P := \{Q_1, \ldots, Q_{N^2}\}$)
- Consider $L = K(N^{-1}P)$
- L contains the N-th torsion field $K(E[N])$
- $L \mid K$ and $L \mid K(E[N])$ are Galois

Kummer Theories - comparison

Classical	**Elliptic Curves**
$\mathbb{G}_m$	E
roots of unity $\zeta_N \in \mu_N$	torsion points $T \in E[N]$
$K(\zeta_N)$	$K(E[N])$
$a \in K^\times$ not root of unity	$P \in E(K)$ not torsion
$\{b \in \overline{K}^\times \mid b^N = a\}$	$\{Q \in E(\overline{K}) \mid NQ = P\}$
$K(\sqrt[N]{a}, \zeta_N)$	$K(N^{-1}P)$
$[K(\sqrt[N]{a}, \zeta_N) : K(\zeta_N)] \sim N$	$[K(N^{-1}P) : K(E[N])] \sim N^2$

Main result

Theorem (D. Lombardo - S. T. (2019))

Assume that $\mathrm{End}_K(E) = \mathbb{Z}$. *There is an explicit constant* C, *depending only on* P *and on the torsion Galois representations associated with* E *such that*

$$\frac{N^2}{[K(N^{-1}P) : K(E[N])]} \qquad \textit{divides} \qquad C$$

for all $N \geq 1$.

Main result

Theorem (D. Lombardo - S. T. (2019))

Assume that $\mathrm{End}_K(E) = \mathbb{Z}$. *There is an explicit constant* C, *depending only on* P *and on the torsion Galois representations associated with* E *such that*

$$\frac{N^2}{[K(N^{-1}P) : K(E[N])]} \qquad \text{divides} \qquad C$$

for all $N \geq 1$.

Already known with a non-explicit constant.

Main result - idea of proof

Elementary field theory gives

$$\frac{N^2}{[K(N^{-1}P):K(E[N])]} =$$

$$= \prod_{\substack{\ell \mid N \\ \ell \text{ prime}}} \underbrace{\frac{\ell^{2n_\ell}}{[K(\ell^{-n_\ell}P):K(E[\ell^{n_\ell}])]}}_{A_\ell(N)} \cdot \underbrace{[K(\ell^{-n_\ell}P) \cap K(E[N]) : K(E[\ell^{n_\ell}])]}_{B_\ell(N)}$$

where $n_\ell = v_\ell(N)$.

Main result - idea of proof

Elementary field theory gives

$$\frac{N^2}{[K(N^{-1}P):K(E[N])]} =$$

$$= \prod_{\substack{\ell \mid N \\ \ell \text{ prime}}} \underbrace{\frac{\ell^{2n_\ell}}{[K(\ell^{-n_\ell}P):K(E[\ell^{n_\ell}])]}}_{A_\ell(N)} \cdot \underbrace{[K(\ell^{-n_\ell}P)\cap K(E[N]):K(E[\ell^{n_\ell}])]}_{B_\ell(N)}$$

where $n_\ell = v_\ell(N)$. We call $A_\ell(N)$ the ℓ-adic failure and $B_\ell(N)$ the adelic failure.

Main result - idea of proof

Goals:

Main result - idea of proof

Goals:

- Show that A_ℓ is bounded as a function of N

Main result - idea of proof

Goals:

- Show that A_ℓ is bounded as a function of N
- $A_\ell = 1$ for almost all primes

Main result - idea of proof

Goals:

- Show that A_ℓ is bounded as a function of N
- $A_\ell = 1$ for almost all primes
- Same for B_ℓ

Main result - idea of proof

Goals:

- Show that A_ℓ is bounded as a function of N
- $A_\ell = 1$ for almost all primes
- Same for B_ℓ
- Everything explicitly!

Proof idea - ℓ-adic failure

Assume that E has no CM.

Proof idea - ℓ-adic failure

Assume that E has no CM. Fix a prime ℓ.

Proof idea - ℓ-adic failure

Assume that E has no CM. Fix a prime ℓ.

- Write $P = \ell^{d_\ell} Q + T$ in $E(K)$, with T torsion and d_ℓ maximal

Proof idea - ℓ-adic failure

Assume that E has no CM. Fix a prime ℓ.

- Write $P = \ell^{d_\ell} Q + T$ in $E(K)$, with T torsion and d_ℓ maximal

Theorem (J. Rouse, N. Jones (2007))

If $d_\ell = 0$ and the ℓ-adic Galois representation associated with E is surjective, (+ extra condition for $\ell = 2$) then $A_\ell(N) = 1$ for every $N > 1$.

Proof idea - ℓ-adic failure

Assume that E has no CM. Fix a prime ℓ.

- Write $P = \ell^{d_\ell} Q + T$ in $E(K)$, with T torsion and d_ℓ maximal

Theorem (J. Rouse, N. Jones (2007))

If $d_\ell = 0$ and the ℓ-adic Galois representation associated with E is surjective, ($+$ extra condition for $\ell = 2$) then $A_\ell(N) = 1$ for every $N > 1$.

- Serre's open image theorem $\implies$ finitely many primes left

Proof idea - ℓ-adic failure (an example)

Problem: d_ℓ may increase when we work over $K(E[\ell^n])$

Proof idea - ℓ-adic failure (an example)

Problem: d_ℓ may increase when we work over $K(E[\ell^n])$

Example

The curve

$$E/\mathbb{Q}: \qquad y^2 + y = x^3 - 216x - 1861 \qquad \textit{(Cremona 17739g1)}$$

has a point

$$P = \left(\frac{23769}{400}, \frac{3529853}{8000}\right) \in E(\mathbb{Q})$$

with $d_3 = 0$.

Proof idea - ℓ-adic failure (an example)

Problem: d_ℓ may increase when we work over $K(E[\ell^n])$

Example

The curve

$$E/\mathbb{Q}: \qquad y^2 + y = x^3 - 216x - 1861 \qquad \textit{(Cremona 17739g1)}$$

has a point

$$P = \left(\frac{23769}{400}, \frac{3529853}{8000}\right) \in E(\mathbb{Q})$$

with $d_3 = 0$.
However, there is a point $Q \in \mathbb{Q}(E[3])$ *such that* $P = 3Q$.

Proof idea - ℓ-adic failure

Using Galois cohomology, we bound A_ℓ in terms of:

- the integer d_ℓ
- "how much" ρ_{ℓ^∞} is not surjective

Proof idea - ℓ-adic failure

Using Galois cohomology, we bound A_ℓ in terms of:

- the integer d_ℓ
- "how much" ρ_{ℓ^∞} is not surjective

Proposition

There is an explicit integer c_ℓ, depending only on the ℓ-adic Galois representation associated with E, such that $A_\ell(N)$ divides $\ell^{4c_\ell+2d_\ell}$ for every $N > 1$.

Proof idea - adelic failure

Let $n_\ell = v_\ell(N)$ and $R = N/\ell^{n_\ell}$.

Proof idea - adelic failure

Let $n_\ell = v_\ell(N)$ and $R = N/\ell^{n_\ell}$.
Recall $B_\ell(N) = [K(\ell^{-n_\ell}P) \cap K(E[N]) : K(E[\ell^{n_\ell}])]$.

Proof idea - adelic failure

Let $n_\ell = v_\ell(N)$ and $R = N/\ell^{n_\ell}$.
Recall $B_\ell(N) = [K(\ell^{-n_\ell}P) \cap K(E[N]) : K(E[\ell^{n_\ell}])]$.

- One can show that

$$B_\ell(N) = [\underbrace{K(\ell^{-n_\ell}P) \cap K(E[R])}_{F} : \underbrace{K(E[\ell^{n_\ell}]) \cap K(E[R])}_{T}]$$

Proof idea - adelic failure

Let $n_\ell = v_\ell(N)$ and $R = N/\ell^{n_\ell}$.
Recall $B_\ell(N) = [K(\ell^{-n_\ell}P) \cap K(E[N]) : K(E[\ell^{n_\ell}])]$.

- One can show that

$$B_\ell(N) = [\underbrace{K(\ell^{-n_\ell}P) \cap K(E[R])}_{F} : \underbrace{K(E[\ell^{n_\ell}]) \cap K(E[R])}_{T}]$$

- If $T = K$ then $B_\ell(N) = 1$

Proof idea - adelic failure

Theorem (F. Campagna, P. Stevenhagen (2018))

There is a finite and explicit set of primes S, depending only on E, such that if $\ell \notin S$, then $T = K$.

Proof idea - adelic failure

Theorem (F. Campagna, P. Stevenhagen (2018))

There is a finite and explicit set of primes S, depending only on E, such that if $\ell \notin S$, then $T = K$.

For all other primes:

Proof idea - adelic failure

Theorem (F. Campagna, P. Stevenhagen (2018))

There is a finite and explicit set of primes S, depending only on E, such that if $\ell \notin S$, then $T = K$.

For all other primes:

- There is a finite extension $\tilde{K} \mid K$, depending only on S, such that working over $\tilde{K}$ we have $T = K$

Proof idea - adelic failure

Theorem (F. Campagna, P. Stevenhagen (2018))

There is a finite and explicit set of primes S, depending only on E, such that if $\ell \notin S$, then $T = K$.

For all other primes:

- There is a finite extension $\tilde{K} \mid K$, depending only on S, such that working over $\tilde{K}$ we have $T = K$
- We have the bound

$$B_\ell(N) \mid \ell^{2c_\ell + 3v_\ell([\tilde{K}:K])}$$

Proof idea - summary

1. Split the "failure of maximality" in ℓ-adic and adelic failures

Proof idea - summary

1. Split the "failure of maximality" in ℓ-adic and adelic failures
2. For most primes things are nice and $A_\ell = B_\ell = 1$
   (direct application of other people's results)

Proof idea - summary

1. Split the "failure of maximality" in ℓ-adic and adelic failures
2. For most primes things are nice and $A_\ell = B_\ell = 1$
   (direct application of other people's results)
3. For other primes, things don't go too bad
   (some extra work to do)

Main result

Theorem (D. Lombardo - S. T. (2019))

Assume that $\mathrm{End}_K(E) = \mathbb{Z}$*. There is an explicit constant* C*, depending only on* P *and on the torsion Galois representations associated with* E *such that*

$$\frac{N^2}{[K(N^{-1}P) : K(E[N])]} \quad \text{divides} \quad C$$

for all $N \geq 1$*.*

Already known with a non-explicit constant.

Future work

- Uniform bounds (done over $\mathbb{Q}$)

Future work

- Uniform bounds (done over $\mathbb{Q}$)
- More points (work in progress)

Future work

- Uniform bounds (done over $\mathbb{Q}$)
- More points (work in progress)
- CM curves, abelian varieties

Future work

- Uniform bounds (done over $\mathbb{Q}$)
- More points (work in progress)
- CM curves, abelian varieties
- More explicit/algorithmic results

Thank you for your attention!