Explicit Isogenies of prime degree over number fields

work in progress with Maarten Derickx

Barinder Singh Banwait

Ruprecht-Karls-Universität Heidelberg

Atelier PARI/GP
Université de Franche-Comté, Besançon
Thursday, 13th January 2022

UNIVERSITÄT HEIDELBERG
ZUKUNFT SEIT 1386

Copyright Disclaimer: Photo credits and attribution are given on the final slide.

I was really looking forward to being there in person this week ...

I was really looking forward to being there in person this week ...

... but France had closed its border to people from the UK unless they had a "motifs impérieux" for travel, and

I was really looking forward to being there in person this week ...

... but France had closed its border to people from the UK unless they had a "motifs impérieux" for travel, and

> *Ces motifs ne permettront pas de se déplacer pour raisons touristiques ou professionnelles*

This *did* get relaxed on 6th January, so I *could* have travelled with last-minute bookings, but then I received this ...

This *did* get relaxed on 6th January, so I *could* have travelled with last-minute bookings, but then I received this ...

NHS

Dear Barinder Banwait
Birth date: 24/11/1986
Test date: 06/01/2022

Your coronavirus PCR test (or other lab test) result is positive. It's likely you had the virus when the test was done.

Self-isolate immediately (including if this is a follow-up test result) from the day your symptoms started, or the test date if you've no symptoms.

This *did* get relaxed on 6th January, so I *could* have travelled with last-minute bookings, but then I received this ...

NHS

Dear Barinder Banwait
Birth date: 24/11/1986
Test date: 06/01/2022

Your coronavirus PCR test (or other lab test) result is positive. It's likely you had the virus when the test was done.

Self-isolate immediately (including if this is a follow-up test result) from the day your symptoms started, or the test date if you've no symptoms.

Fortunately it has been mostly mild.

Introduction

Rational Isogenies

Rational Isogenies

Let E_1, E_2 be two elliptic curves over a number field K. Write $G_K := \mathrm{Gal}(\overline{K}/K)$.

Rational Isogenies

Let E_1, E_2 be two elliptic curves over a number field K. Write $G_K := \mathrm{Gal}(\overline{K}/K)$.

Definition

- An isogeny $\phi : E_1 \to E_2$ is a non-constant morphism of curves which

Rational Isogenies

Let E_1, E_2 be two elliptic curves over a number field K. Write $G_K := \mathrm{Gal}(\overline{K}/K)$.

Definition

- An isogeny $\phi : E_1 \to E_2$ is a non-constant morphism of curves which
  - maps O_{E_1} to O_{E_2};

Rational Isogenies

Let E_1, E_2 be two elliptic curves over a number field K. Write $G_K := \mathrm{Gal}(\overline{K}/K)$.

Definition

- An isogeny $\phi : E_1 \to E_2$ is a non-constant morphism of curves which
  - ◎ maps O_{E_1} to O_{E_2};
  - ⇔ induces a group homomorphism from $E_1(\overline{K})$ to $E_2(\overline{K})$;

Rational Isogenies

Let E_1, E_2 be two elliptic curves over a number field K. Write $G_K := \mathrm{Gal}(\overline{K}/K)$.

Definition

- An isogeny $\phi : E_1 \to E_2$ is a non-constant morphism of curves which
  - ◎ maps O_{E_1} to O_{E_2};
  - ⇔ induces a group homomorphism from $E_1(\overline{K})$ to $E_2(\overline{K})$;
  - ⇔ has finite kernel.

Rational Isogenies

Let E_1, E_2 be two elliptic curves over a number field K. Write $G_K := \mathrm{Gal}(\overline{K}/K)$.

Definition

- An isogeny $\phi : E_1 \to E_2$ is a non-constant morphism of curves which
  - maps O_{E_1} to O_{E_2};
  - $\Leftrightarrow$ induces a group homomorphism from $E_1(\overline{K})$ to $E_2(\overline{K})$;
  - $\Leftrightarrow$ has finite kernel.
- The degree of ϕ $= |\ker(\phi)| = [\overline{K}(E_1) : \phi^* \overline{K}(E_2)]$.

Rational Isogenies

Let E_1, E_2 be two elliptic curves over a number field K. Write $G_K := \mathrm{Gal}(\overline{K}/K)$.

Definition

- An isogeny $\phi : E_1 \to E_2$ is a non-constant morphism of curves which
  - maps O_{E_1} to O_{E_2};
  - $\Leftrightarrow$ induces a group homomorphism from $E_1(\overline{K})$ to $E_2(\overline{K})$;
  - $\Leftrightarrow$ has finite kernel.
- The degree of ϕ $= |\ker(\phi)| = [\overline{K}(E_1) : \phi^*\overline{K}(E_2)]$.
- ϕ is K-rational if it is compatible with the G_K-action on E_1 and E_2; that is, if the following diagram commutes for all $\sigma \in G_K$:

$$\begin{tikzcd} E_1 \arrow[r, "\phi"] \arrow[d, "\sigma"'] & E_2 \arrow[d, "\sigma"] \\ E_1 \arrow[r, "\phi"] & E_2 \end{tikzcd}$$

Rational Isogenies

Let E_1, E_2 be two elliptic curves over a number field K. Write $G_K := \mathrm{Gal}(\overline{K}/K)$.

Definition

- An isogeny $\phi : E_1 \to E_2$ is a non-constant morphism of curves which
  - ◎ maps O_{E_1} to O_{E_2};
  - $\Leftrightarrow$ induces a group homomorphism from $E_1(\overline{K})$ to $E_2(\overline{K})$;
  - $\Leftrightarrow$ has finite kernel.
- The degree of ϕ $= |\ker(\phi)| = [\overline{K}(E_1) : \phi^*\overline{K}(E_2)]$.
- ϕ is K-rational if it is compatible with the G_K-action on E_1 and E_2; that is, if the following diagram commutes for all $\sigma \in G_K$:

$$\begin{tikzcd} E_1 \arrow[r, "\phi"] \arrow[d, "\sigma"'] & E_2 \arrow[d, "\sigma"] \\ E_1 \arrow[r, "\phi"] & E_2 \end{tikzcd}$$

Equivalently, ϕ is K-rational if $\ker(\phi)$ is G_K-stable.

Rational Isogenies

Let E_1, E_2 be two elliptic curves over a number field K. Write $G_K := \mathrm{Gal}(\overline{K}/K)$.

Definition

- An isogeny $\phi : E_1 \to E_2$ is a non-constant morphism of curves which
  - ◎ maps O_{E_1} to O_{E_2};
  - $\Leftrightarrow$ induces a group homomorphism from $E_1(\overline{K})$ to $E_2(\overline{K})$;
  - $\Leftrightarrow$ has finite kernel.
- The degree of ϕ $= |\ker(\phi)| = [\overline{K}(E_1) : \phi^*\overline{K}(E_2)]$.
- ϕ is K-rational if it is compatible with the G_K-action on E_1 and E_2; that is, if the following diagram commutes for all $\sigma \in G_K$:

$$\begin{tikzcd} E_1 \arrow[r, "\phi"] \arrow[d, "\sigma"'] & E_2 \arrow[d, "\sigma"] \\ E_1 \arrow[r, "\phi"] & E_2 \end{tikzcd}$$

  Equivalently, ϕ is K-rational if $\ker(\phi)$ is G_K-stable.
- ϕ is said to be cyclic if $\ker(\phi)$ is a cyclic group.

Isogeny classes are finite over number fields

Isogeny classes are finite over number fields

Theorem (Shafarevich, 1962)

Let E/K be an elliptic curve over a number field. Then there are only finitely many elliptic curves E'/K which are K-isogenous to E.

Isogeny classes are finite over number fields

Theorem (Shafarevich, 1962)

Let E/K be an elliptic curve over a number field. Then there are only finitely many elliptic curves E'/K which are K-isogenous to E.

Fact

Every isogeny is the composition of a cyclic isogeny with the multiplication-by-m map for some $m \geq 1$.

Isogeny classes are finite over number fields

Theorem (Shafarevich, 1962)

Let E/K be an elliptic curve over a number field. Then there are only finitely many elliptic curves E'/K which are K-isogenous to E.

Fact

Every isogeny is the composition of a cyclic isogeny with the multiplication-by-m map for some $m \geq 1$.

So between any two elliptic curves in the isogeny class of E, there is a unique minimal cyclic isogeny degree between them.

These minimal cyclic isogeny degrees are implemented in PARI/GP as `ellisomat`.

These minimal cyclic isogeny degrees are implemented in PARI/GP as `ellisomat`.

```
? nf = nfinit(a^2 - 2);
? ell = ellinit([a,-1,0,18,46],nf);
? [L,M] = ellisomat(ell);
cpu time = 125 ms, real time = 163 ms.
? M[,1]
%8 = [1, 2, 4, 4, 3, 3, 6, 6, 12, 12, 12, 12]~
```

These minimal cyclic isogeny degrees are implemented in PARI/GP as `ellisomat`.

```
? nf = nfinit(a^2 - 2);
? ell = ellinit([a,-1,0,18,46],nf);
? [L,M] = ellisomat(ell);
cpu time = 125 ms, real time = 163 ms.
? M[,1]
%8 = [1, 2, 4, 4, 3, 3, 6, 6, 12, 12, 12, 12]~
```

The degree computation is based on Billerey's algorithm for computing isogenies of prime degree for a fixed elliptic curve E/K.

Nicolas Billerey

Uniform isogeny primes?

Definition

For a number field K, a prime p is called an **isogeny prime for** K if there exists an elliptic curve over K which admits a K-rational p-isogeny. We write the set of such primes as $\mathrm{IsogPrimeDeg}(K)$.

Uniform isogeny primes?

Definition

For a number field K, a prime p is called an **isogeny prime for** K if there exists an elliptic curve over K which admits a K-rational p-isogeny. We write the set of such primes as $\mathrm{IsogPrimeDeg}(K)$.

By the theory of CM, $\mathrm{IsogPrimeDeg}(K)$ is infinite if K contains the Hilbert class field of an imaginary quadratic field.

Uniform isogeny primes?

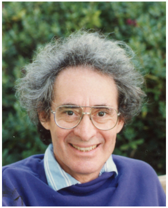
Definition

For a number field K, a prime p is called an **isogeny prime for** K if there exists an elliptic curve over K which admits a K-rational p-isogeny. We write the set of such primes as $\mathrm{IsogPrimeDeg}(K)$.

By the theory of CM, $\mathrm{IsogPrimeDeg}(K)$ is infinite if K contains the Hilbert class field of an imaginary quadratic field.

Theorem (Mazur, 1978)

$$\mathrm{IsogPrimeDeg}(\mathbb{Q}) = \{2, 3, 5, 7, 11, 13, 17, 19, 37, 43, 67, 163\}$$

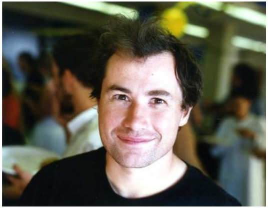


Barry C. Mazur

Theorem (Momose + Merel, 1995)

Assume GRH. Then $\mathrm{IsogPrimeDeg}(K)$ *is finite if and only if* K *does not contain the Hilbert class field of an imaginary quadratic field.*

Fumiyuki Momose



Löic Merel

Isogeny Prime v1

Computing IsogPrimeDeg(K)?

Computing IsogPrimeDeg(K)?

Theorem (B.-Derickx)

Let K be a number field which does not contain the Hilbert class field of an imaginary quadratic field. Then there is an algorithm which computes a superset of $\mathrm{IsogPrimeDeg}(K)$ *as the union of three sets:*

$$\mathrm{IsogPrimeDeg}(K) \subseteq \mathrm{PreTypeOneTwoPrimes}(K) \cup \mathrm{TypeOnePrimes}(K) \cup \mathrm{TypeTwoPrimes}(K).$$

With Maarten Derickx in West London last week

Isogeny types

Let E/K be an elliptic curve over a number field which admits a K-rational p-isogeny.

Isogeny types

Let E/K be an elliptic curve over a number field which admits a K-rational p-isogeny. Let λ denote the isogeny character:

Isogeny types

Let E/K be an elliptic curve over a number field which admits a K-rational p-isogeny. Let λ denote the isogeny character:

$$\lambda : G_K \longrightarrow \operatorname{Aut} V(\overline{K}) \cong \mathbb{F}_p^\times ,$$

Isogeny types

Let E/K be an elliptic curve over a number field which admits a K-rational p-isogeny. Let λ denote the isogeny character:

$$\lambda : G_K \longrightarrow \mathrm{Aut}\, V(\overline{K}) \cong \mathbb{F}_p^\times,$$

where V is the kernel of the isogeny

Isogeny types

Let E/K be an elliptic curve over a number field which admits a K-rational p-isogeny. Let λ denote the isogeny character:

$$\lambda : G_K \longrightarrow \operatorname{Aut} V(\overline{K}) \cong \mathbb{F}_p^\times,$$

where V is the kernel of the isogeny, which can be thought of as a 1d G_K-representation.

Isogeny types

Let E/K be an elliptic curve over a number field which admits a K-rational p-isogeny. Let λ denote the isogeny character:

$$\lambda : G_K \longrightarrow \operatorname{Aut} V(\overline{K}) \cong \mathbb{F}_p^\times ,$$

where V is the kernel of the isogeny, which can be thought of as a 1d G_K-representation.

Theorem (Momose, watered-down)

Let K be a number field which does not contain the HCF of an IQF. Then there exists a constant $C_0 = C_0(K)$ such that for any prime $p > C_0$, and for any elliptic curve admitting a K-rational p-isogeny, the isogeny character λ falls into one of the following two types:

Isogeny types

Let E/K be an elliptic curve over a number field which admits a K-rational p-isogeny. Let λ denote the isogeny character:

$$\lambda : G_K \longrightarrow \operatorname{Aut} V(\overline{K}) \cong \mathbb{F}_p^\times,$$

where V is the kernel of the isogeny, which can be thought of as a 1d G_K-representation.

Theorem (Momose, watered-down)

Let K be a number field which does not contain the HCF of an IQF. Then there exists a constant $C_0 = C_0(K)$ such that for any prime $p > C_0$, and for any elliptic curve admitting a K-rational p-isogeny, the isogeny character λ falls into one of the following two types:

Type 1. λ^{12} *or* $(\lambda\theta_p^{-1})^{12}$ *is unramified ($\theta_p =$mod-p cyclotomic character).*

Isogeny types

Let E/K be an elliptic curve over a number field which admits a K-rational p-isogeny. Let λ denote the isogeny character:

$$\lambda : G_K \longrightarrow \mathrm{Aut}\, V(\overline{K}) \cong \mathbb{F}_p^\times,$$

where V is the kernel of the isogeny, which can be thought of as a 1d G_K-representation.

Theorem (Momose, watered-down)

Let K be a number field which does not contain the HCF of an IQF. Then there exists a constant $C_0 = C_0(K)$ such that for any prime $p > C_0$, and for any elliptic curve admitting a K-rational p-isogeny, the isogeny character λ falls into one of the following two types:

Type 1. λ^{12} *or* $(\lambda\theta_p^{-1})^{12}$ *is unramified* ($\theta_p =$*mod-p cyclotomic character).*

Type 2. $\lambda^{12} = \theta_p^6$ *and* $p \equiv 3 \pmod 4$.

These two special types of λ arise from the following Lemma.

These two special types of λ arise from the following Lemma. By class field theory, we can identify λ as a character of $I_K(p)$, ideals of K coprime to p.

These two special types of λ arise from the following Lemma. By class field theory, we can identify λ as a character of $I_K(p)$, ideals of K coprime to p.

LEMMA 1. *Assume that k is a Galois extension of $\mathbf{Q}$ and that the rational prime p is unramified in k. Then for a fixed prime $\mathfrak{p}$ of k lying over p, we have integers a_σ, $0 \leqslant a_\sigma \leqslant 12$, for $\sigma \in \mathrm{Gal}(k/\mathbf{Q})$ such that*

$$\lambda^{12}((\alpha)) \equiv \alpha^{\varepsilon} \pmod{\mathfrak{p}}$$

for $\varepsilon = \Sigma_\sigma a_\sigma \sigma$ and $\alpha \in k^\times$ prime to p.

These two special types of λ arise from the following Lemma. By class field theory, we can identify λ as a character of $I_K(p)$, ideals of K coprime to p.

LEMMA 1. *Assume that k is a Galois extension of $\mathbf{Q}$ and that the rational prime p is unramified in k. Then for a fixed prime $\mathfrak{p}$ of k lying over p, we have integers a_σ, $0 \leqslant a_\sigma \leqslant 12$, for $\sigma \in \mathrm{Gal}(k/\mathbf{Q})$ such that*

$$\lambda^{12}((\alpha)) \equiv \alpha^{\varepsilon} \pmod{\mathfrak{p}}$$

for $\varepsilon = \Sigma_\sigma a_\sigma \sigma$ and $\alpha \in k^\times$ prime to p.

We show that the same result holds in the non-Galois setting, by replacing $\mathrm{Gal}(K/\mathbb{Q})$ with $\mathrm{Hom}(K, K^g)$, where K^g is the Galois closure of K.

These two special types of λ arise from the following Lemma. By class field theory, we can identify λ as a character of $I_K(p)$, ideals of K coprime to p.

LEMMA 1. *Assume that k is a Galois extension of $\mathbf{Q}$ and that the rational prime p is unramified in k. Then for a fixed prime $\mathfrak{p}$ of k lying over p, we have integers a_σ, $0 \leqslant a_\sigma \leqslant 12$, for $\sigma \in \mathrm{Gal}(k/\mathbf{Q})$ such that*

$$\lambda^{12}((\alpha)) \equiv \alpha^{\varepsilon} \pmod{\mathfrak{p}}$$

for $\varepsilon = \Sigma_\sigma a_\sigma \sigma$ and $\alpha \in k^\times$ prime to p.

We show that the same result holds in the non-Galois setting, by replacing $\mathrm{Gal}(K/\mathbb{Q})$ with $\mathrm{Hom}(K, K^g)$, where K^g is the Galois closure of K.

By fixing an ordering of the embeddings in $\Sigma := \mathrm{Hom}(K, K^g)$, we can think of ε as a tuple $(a_\sigma)_{\sigma \in \Sigma}$, called the isogeny signature.

These two special types of λ arise from the following Lemma. By class field theory, we can identify λ as a character of $I_K(p)$, ideals of K coprime to p.

LEMMA 1. *Assume that k is a Galois extension of $\mathbf{Q}$ and that the rational prime p is unramified in k. Then for a fixed prime $\mathfrak{p}$ of k lying over p, we have integers a_σ, $0 \leqslant a_\sigma \leqslant 12$, for $\sigma \in \mathrm{Gal}(k/\mathbf{Q})$ such that*

$$\lambda^{12}((\alpha)) \equiv \alpha^{\varepsilon} \pmod{\mathfrak{p}}$$

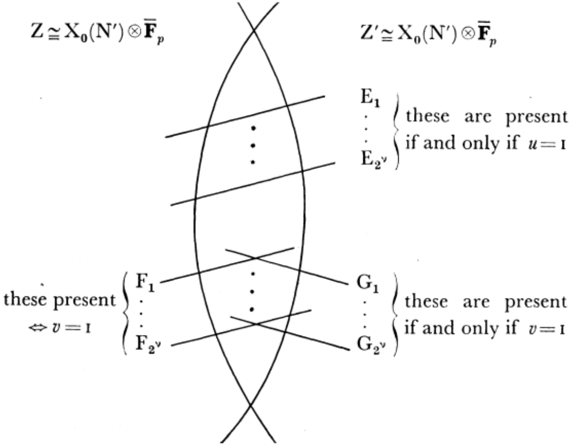
for $\varepsilon = \Sigma_\sigma a_\sigma \sigma$ and $\alpha \in k^\times$ prime to p.

We show that the same result holds in the non-Galois setting, by replacing $\mathrm{Gal}(K/\mathbb{Q})$ with $\mathrm{Hom}(K, K^g)$, where K^g is the Galois closure of K.

By fixing an ordering of the embeddings in $\Sigma := \mathrm{Hom}(K, K^g)$, we can think of ε as a tuple $(a_\sigma)_{\sigma \in \Sigma}$, called the isogeny signature.

REMARK 1. The integers $a_\mathfrak{P}$'s take the values $0, 12; 4, 8$ (only if the modular invariant $j(E) \equiv 0 \pmod{\mathfrak{p}}$ and $p \equiv 2 \pmod 3$); 6 (only if $j(E) \equiv 1728 \pmod{\mathfrak{p}}$ and $p \equiv 3 \pmod 4$) (cf. [Ma1], Chap. 3; [Ma2]).

We obtain the following picture for the reduction modulo p of $X_0(N)$:



From Mazur and Rapoport's Appendix to Mazur's 1977 paper. The E components arise from $j = 1728$ elliptic curves, the F and G from $j = 0$.

λ of Type 1 means $\varepsilon = (0, \cdots, 0)$ or $(12, \cdots, 12)$

λ of Type 1 means $\varepsilon = (0, \cdots, 0)$ or $(12, \cdots, 12)$

λ of Type 2 means $\varepsilon = (6, \cdots, 6)$

$$\lambda \text{ of Type 1 means } \varepsilon = (0, \cdots, 0) \text{ or } (12, \cdots, 12)$$

$$\lambda \text{ of Type 2 means } \varepsilon = (6, \cdots, 6)$$

For the other signatures ε one can construct a non-zero integer $ABC(\varepsilon, \mathfrak{q})$ (for prime ideals $\mathfrak{q}$ of K) which multiplicatively bounds the isogeny primes with that signature.

TypeOnePrimes

Let E/K be an elliptic curve with a K-rational p-isogeny of Type 1. Replacing this isogeny with its dual if necessary, we may suppose that $\lambda^{12h_K} = 1$, i.e., $\epsilon = (0, \cdots, 0)$.

TypeOnePrimes

Let E/K be an elliptic curve with a K-rational p-isogeny of Type 1. Replacing this isogeny with its dual if necessary, we may suppose that $\lambda^{12h_K} = 1$, i.e., $\epsilon = (0, \cdots, 0)$.

Case 1. E has potentially good reduction at $\mathfrak{q}$.

TypeOnePrimes

Let E/K be an elliptic curve with a K-rational p-isogeny of Type 1. Replacing this isogeny with its dual if necessary, we may suppose that $\lambda^{12h_K} = 1$, i.e., $\epsilon = (0, \cdots, 0)$.

Case 1. **E has potentially good reduction at $\mathfrak{q}$.**

Then $\lambda(\mathrm{Frob}_{\mathfrak{q}}) \equiv \beta$ for some root β of the characteristic polynomial of Frobenius of an elliptic curve over $\mathbb{F}_{\mathfrak{q}}$.

TypeOnePrimes

Let E/K be an elliptic curve with a K-rational p-isogeny of Type 1. Replacing this isogeny with its dual if necessary, we may suppose that $\lambda^{12h_K} = 1$, i.e., $\epsilon = (0, \cdots, 0)$.

Case 1. E has potentially good reduction at $\mathfrak{q}$.

Then $\lambda(\mathrm{Frob}_{\mathfrak{q}}) \equiv \beta$ for some root β of the characteristic polynomial of Frobenius of an elliptic curve over $\mathbb{F}_{\mathfrak{q}}$.

$$p \mid \mathrm{Nm}(\beta^{12h_{\mathfrak{q}}} - 1)$$

i.e. we can multiplicatively bound this case.

Case 2. E has potentially multiplicative reduction at $\mathfrak{q}$.

Case 2. **E has potentially multiplicative reduction at $\mathfrak{q}$.**
Writing x for the non-cuspidal K-point on $X_0(p)$ corresponding to E, we have that

$$x_{/\mathbb{F}_\mathfrak{q}} = \infty_{/\mathbb{F}_\mathfrak{q}} \text{ or } 0_{/\mathbb{F}_\mathfrak{q}}.$$

Case 2. E has potentially multiplicative reduction at $\mathfrak{q}$.
Writing x for the non-cuspidal K-point on $X_0(p)$ corresponding to E, we have that

$$x_{/\mathbb{F}_\mathfrak{q}} = \infty_{/\mathbb{F}_\mathfrak{q}} \text{ or } 0_{/\mathbb{F}_\mathfrak{q}}.$$

One then proves in each case that

$$\lambda^2(\mathrm{Frob}_\mathfrak{q}) \equiv 1 \text{ or } \mathrm{Nm}(\mathfrak{q})^2.$$

Case 2. E has potentially multiplicative reduction at $\mathfrak{q}$.
Writing x for the non-cuspidal K-point on $X_0(p)$ corresponding to E, we have that

$$x_{/\mathbb{F}_{\mathfrak{q}}} = \infty_{/\mathbb{F}_{\mathfrak{q}}} \text{ or } 0_{/\mathbb{F}_{\mathfrak{q}}}.$$

One then proves in each case that

$$\lambda^2(\mathrm{Frob}_{\mathfrak{q}}) \equiv 1 \text{ or } \mathrm{Nm}(\mathfrak{q})^2.$$

The latter case yields

$$1 = \lambda^{12h_{\mathfrak{q}}}(\mathrm{Frob}_{\mathfrak{q}}) \equiv \mathrm{Nm}(\mathfrak{q})^{12h_{\mathfrak{q}}} \pmod{p}$$
$$\Rightarrow p \mid \mathrm{Nm}(\mathfrak{q})^{12h_{\mathfrak{q}}} - 1.$$

Case 2. E has potentially multiplicative reduction at $\mathfrak{q}$.
Writing x for the non-cuspidal K-point on $X_0(p)$ corresponding to E, we have that

$$x_{/\mathbb{F}_\mathfrak{q}} = \infty_{/\mathbb{F}_\mathfrak{q}} \text{ or } 0_{/\mathbb{F}_\mathfrak{q}}.$$

One then proves in each case that

$$\lambda^2(\mathrm{Frob}_\mathfrak{q}) \equiv 1 \text{ or } \mathrm{Nm}(\mathfrak{q})^2.$$

The latter case yields

$$\begin{aligned} &1 = \lambda^{12h_\mathfrak{q}}(\mathrm{Frob}_\mathfrak{q}) \equiv \mathrm{Nm}(\mathfrak{q})^{12h_\mathfrak{q}} \pmod p \\ &\Rightarrow p \mid \mathrm{Nm}(\mathfrak{q})^{12h_\mathfrak{q}} - 1. \end{aligned}$$

In the first case: if any of the embedded points x^σ specializes to $0_{/\mathbb{F}_\mathfrak{q}}$, then we again get a non-zero multiplicative bound.

Problem Case

The $\mathbb{Q}$-rational point $(x^\sigma)_{\sigma\in\Sigma}$ on the d-th symmetric power modular curve $X_0(p)^{(d)}$ specializes to $(\infty, \cdots, \infty)$ at $\mathfrak{q}$.

Problem Case

The $\mathbb{Q}$-rational point $(x^\sigma)_{\sigma \in \Sigma}$ on the d-th symmetric power modular curve $X_0(p)^{(d)}$ specializes to $(\infty, \cdots, \infty)$ at $\mathfrak{q}$.

Define the map

$$\begin{aligned} f_p^{(d)} : \ X_0(p)^{(d)}_{\mathrm{sm},/\mathbb{Z}} &\longrightarrow \quad J_0(p)_{/\mathbb{Z}} \quad \longrightarrow \quad \tilde{J}_{/\mathbb{Z}} \\ D \quad &\longmapsto [D - d(\infty)] \longmapsto [D - d(\infty)] \pmod{\gamma_{\mathfrak{J}} J_0(p)} \end{aligned}$$

Problem Case

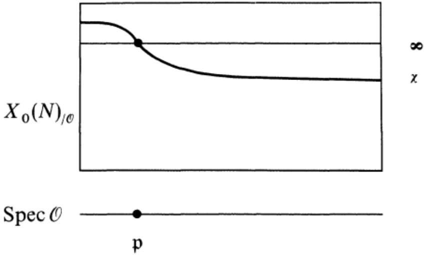
The $\mathbb{Q}$-rational point $(x^\sigma)_{\sigma\in\Sigma}$ on the d-th symmetric power modular curve $X_0(p)^{(d)}$ specializes to $(\infty,\cdots,\infty)$ at $\mathfrak{q}$.

Define the map

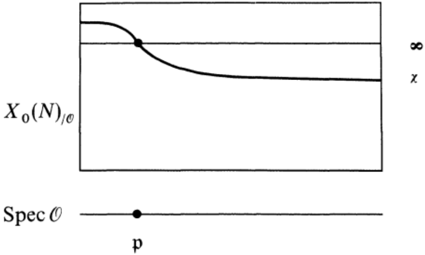
$$\begin{aligned} f_p^{(d)}:\ X_0(p)^{(d)}_{\mathrm{sm},/\mathbb{Z}} &\longrightarrow \quad J_0(p)_{/\mathbb{Z}} \quad \longrightarrow \quad \tilde{J}_{/\mathbb{Z}} \\ D \quad &\longmapsto [D-d(\infty)] \longmapsto [D-d(\infty)] \pmod{\gamma_{\mathfrak{I}} J_0(p)} \end{aligned}$$

By an analogue of **Mazur's specialization lemma**, we obtain that $f(x^\sigma) = f(\infty,\cdots,\infty)$.

We have, therefore, the following state of affairs: the two $\mathcal{O}$-sections of $X_0(N)$, $x_{/\mathcal{O}}$ and $\infty_{/\mathcal{O}}$, "cross" at $\mathfrak{p}$, and map to the same section of A under $f_{/\mathcal{O}}$ (the zero-section). But this contradicts the fact that f is a formal immersion at $\infty_{/k(\mathfrak{p})}$.



We have, therefore, the following state of affairs: the two $\mathcal{O}$-sections of $X_0(N)$, $x_{/\mathcal{O}}$ and $\boldsymbol{\infty}_{/\mathcal{O}}$, "cross" at $\mathfrak{p}$, and map to the same section of A under $f_{/\mathcal{O}}$ (the zero-section). But this contradicts the fact that f is a formal immersion at $\boldsymbol{\infty}_{/k(\mathfrak{p})}$.



We conclude that f is *not* a formal immersion at $(\infty, \cdots, \infty)$.

The set of such ps is very small and can be explicitly bounded.

Proposition 5.3. *Let* $H \subseteq (\mathbb{Z}/p\mathbb{Z})^\times/\{\pm 1\}$ *be a subgroup. Let* $\ell \neq p$ *be a prime and consider* $t = t_1(t_0)$ *as in Proposition 5.1 when* ℓ *is odd, or* t *as in Corollary 5.2 when* $\ell = 2$. *Then* $t \circ \iota$ *is a formal immersion at all* $\bar{x}_H \in X_H^{(d)}(\mathbb{F}_\ell)$ *that are sums of images of rational cusps on* $X_1(p)$*, if for all partitions* $d = n_1 + \ldots + n_m$ *with* $n_1 \geq \cdots \geq n_m$ *and all* m*-tuples* $(d_1 = 1, d_2, \ldots, d_m)$ *of integers representing pairwise distinct elements of* H*, the* d *Hecke operators*

$$(T_i \langle d_j \rangle t)_{\substack{j=1,\ldots,m \\ i=1,\ldots,n_j}} \tag{5.1}$$

are $\mathbb{F}_\ell$*-linearly independent in* $\mathbb{T} \otimes \mathbb{F}_\ell$*, where* $\mathbb{T}$ *is considered as a subalgebra of* $\mathrm{End}_{\mathbb{Q}}(J_H)$.

Maarten Derickx

Sheldon Kamienny

William Stein

Michael Stoll

```python
def get_bad_formal_immersion_data(d):
    """
    This is the Oesterlé for type 1 primes with modular symbols main routine.
    The computation is actually a two step rocket. First Proposition 6.8 of
    Derickx-Kamienny-Stein-Stoll is used to replace Parents polynomial of
    degree 6 bound by something reasonable, and then Corollary 6.4 is used
    to go from something reasonable to the exact list.
    """
    assert d > 0

    p_todo = [int(p) for p in prime_range(11)]
    p_done = {}
    q_to_bad_p = {}

    M = get_M(d)[0]

    for p in prime_range(11, 2 * M * d):
        # first do a relatively cheap test
        if is_formall_immersion_fast(d, p):
            continue
        # this is more expensive
        is_formall = is_formall_immersion(d, p)
        if is_formall:
            if is_formall > 1:
                p_done[int(p)] = is_formall
        else:
            p_todo.append(int(p))

    for p, q_prod in p_done.items():
        for q in prime_divisors(q_prod):
            q_to_bad_p[int(q)] = int(q_to_bad_p.get(q, 1) * p)

    return p_todo, q_to_bad_p
```

TypeTwoPrimes

Condition CC (Momose + B.-Derickx)

Let K be a number field, and E/K an elliptic curve admitting a K-rational p-isogeny of Type 2.

TypeTwoPrimes

Condition CC (Momose + B.-Derickx)

Let K be a number field, and E/K an elliptic curve admitting a K-rational p-isogeny of Type 2. Let q be a rational prime admitting a prime ideal $\mathfrak{q} \mid q$ of residue degree f satisfying:

TypeTwoPrimes

Condition CC (Momose + B.-Derickx)

Let K be a number field, and E/K an elliptic curve admitting a K-rational p-isogeny of Type 2. Let q be a rational prime admitting a prime ideal $\mathfrak{q} \mid q$ of residue degree f satisfying:

1. *f is odd;*
2. $q^f < p/4$;
3. $q^{2f} + q^f + 1 \not\equiv 0 \pmod{p}$.

TypeTwoPrimes

Condition CC (Momose + B.-Derickx)

Let K be a number field, and E/K an elliptic curve admitting a K-rational p-isogeny of Type 2. Let q be a rational prime admitting a prime ideal $\mathfrak{q} \mid q$ of residue degree f satisfying:

1. *f is odd;*
2. *$q^f < p/4$;*
3. *$q^{2f} + q^f + 1 \not\equiv 0 \pmod{p}$.*

Then q does not split in $\mathbb{Q}(\sqrt{-p})$.

TypeTwoPrimes

Condition CC (Momose + B.-Derickx)

Let K be a number field, and E/K an elliptic curve admitting a K-rational p-isogeny of Type 2. Let q be a rational prime admitting a prime ideal $\mathfrak{q} \mid q$ of residue degree f satisfying:

1. *f is odd;*
2. *$q^f < p/4$;*
3. *$q^{2f} + q^f + 1 \not\equiv 0 \pmod{p}$.*

Then q does not split in $\mathbb{Q}(\sqrt{-p})$.

Proposition (B.-Derickx)

Assume GRH. Let K be a number field of degree d, and E/K an elliptic curve possessing a K-rational p-isogeny, for p a Type 2 prime. Then p satisfies

$$p \leq (8d\log(12p) + 16\log(\Delta_K) + 10d + 6)^4.$$

In particular, there are only finitely many primes p as above.

A cubic example

From Superset to Set

Let's run the algorithm on $\mathbb{Q}(\zeta_7)^+$

From Superset to Set

Let's run the algorithm on $\mathbb{Q}(\zeta_7)^+$; we get a superset of

$$\mathrm{PrimesUpTo}(43) \cup \{67, 73, 163\}.$$

From Superset to Set

Let's run the algorithm on $\mathbb{Q}(\zeta_7)^+$; we get a superset of

$$\mathrm{PrimesUpTo}(43) \cup \{67, 73, 163\}.$$

How to determine which of these are actually in $\mathrm{IsogPrimeDeg}(\mathbb{Q}(\zeta_7)^+)$?

From Superset to Set

Let's run the algorithm on $\mathbb{Q}(\zeta_7)^+$; we get a superset of

$$\mathrm{PrimesUpTo}(43) \cup \{67, 73, 163\}.$$

How to determine which of these are actually in $\mathrm{IsogPrimeDeg}(\mathbb{Q}(\zeta_7)^+)$? The main ingredient is

Theorem (Box-Gajović-Goodman, 2021)

*For $N \in \{53, 57, 61, 65, 67, 73\}$, the set of cubic points on $X_0(N)$ is finite and listed in Section 5 of [**?**].*

Josha Box

Stevan Gajović

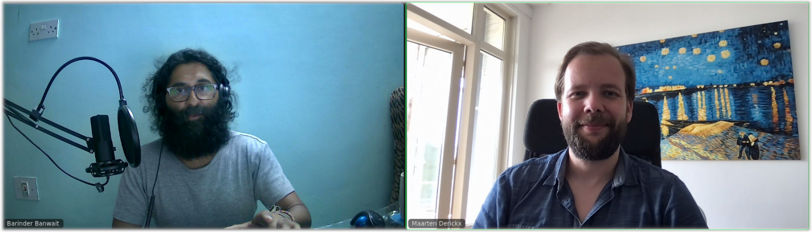
Pip Goodman

The first cubic case of IsogPrimeDeg

Theorem (B.-Derickx)

Assuming GRH,

$$\mathrm{IsogPrimeDeg}(\mathbb{Q}(\zeta_7)^+) = \mathrm{IsogPrimeDeg}(\mathbb{Q})$$



Questions

Question

Can Isogeny Primes v2 be implemented in PARI/GP?

Question

How can checking Type 2 primes be made much faster?