# Quadratic Isogeny Primes

github.com/barinderbanwait/quadratic_isogeny_primes

arxiv.org/abs/2101.02673 - submitted

Barinder Singh Banwait

Harish-Chandra Research Institute

MEGA 2021

Virtually in Tromsø, Norway

June 07-11, 2021


# Isogenies

# 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 $: E_1 \; ! \; E_2$ 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 $O_{E_2}$;
- induces a group homomorphism from $E_1(\overline{K})$ to $E_2(\overline{K})$;
- has finite kernel.

The degree of $\phi = |\ker(\phi)| = [\overline{K}(E_1) : \phi^*\overline{K}(E_2)]$.

# 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 $O_{E_2}$;
- induces a group homomorphism from $E_1(\overline{K})$ to $E_2(\overline{K})$;
- has finite kernel.

The degree of $\phi = |\ker(\phi)| = [\overline{K}(E_1) : \phi^*\overline{K}(E_2)]$.

$\phi$ is said to be $K$-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 $\sigma \in G_K$:

$$\begin{array}{ccc} E_1 & \longrightarrow & E_2 \\ \downarrow & & \downarrow \\ E_1 & \longrightarrow & E_2 \end{array}$$

# Isogenies = Kernel

# Isogenies = Kernel

**Fact**

*Let $E/K$ be an elliptic curve over a number field. Then there is a bijection*

# Isogenies = Kernel

**Fact**

*Let $E/K$ be an elliptic curve over a number field. Then there is a bijection*

$$\{K\text{-rational isogenies from } E\} \to \{G_K\text{-invariant finite subgroups of } E(\overline{K})\}$$
$$\phi \mapsto \ker \phi$$
$$\phi_C : E \to E/C \qquad [C :$$

# Isogenies = Kernel

**Fact**

*Let $E/K$ be an elliptic curve over a number field. Then there is a bijection*

$$\{K\text{-rational isogenies from } E\} \to \{G_K\text{-invariant finite subgroups of } E(\overline{K})\}$$
$$\varphi \mapsto \ker$$
$$\varphi_C : E \to E/C \qquad [C:$$

**Slogan**

You can identify an isogeny with its kernel.

# The Dream

**Goal**

"Understand rational isogenies."

# The Dream

**Goal**

"Understand rational isogenies."

Since we can identify isogenies with their kernels,

# The Dream

**Goal**

"Understand rational isogenies."

Since we can identify isogenies with their kernels, which are finite abelian groups,

# The Dream

**Goal**

"Understand rational isogenies."

Since we can identify isogenies with their kernels, which are finite abelian groups, which break up as a direct sum of cyclic groups,

# The Dream

**Goal**

"Understand rational isogenies."

Since we can identify isogenies with their kernels, which are finite abelian groups, which break up as a direct sum of cyclic groups, the above goal reduces to

**Reduced Goal**

"Understand rational isogenies with cyclic kernel."

Call these cyclic $K$-isogenies.

# The Dream made precise

**Question**

*For a number field $K$, what possible degrees arise as the degree of a $K$-rational cyclic isogeny between elliptic curves over $K$?*

# The Dream made precise

**Question**

*For a number field $K$, what possible degrees arise as the degree of a $K$-rational cyclic isogeny between elliptic curves over $K$?*

Let's call this set of possible degrees $\mathrm{IsogCyclicDeg}(K)$.

# The Dream made precise

**Question**

*For a number field $K$, what possible degrees arise as the degree of a $K$-rational cyclic isogeny between elliptic curves over $K$?*

Let's call this set of possible degrees $\mathrm{IsogCyclicDeg}(K)$.

We write $\mathrm{IsogPrimeDeg}(K)$ for the primes in this set, and call them isogeny primes for $K$.

# The Dream made precise

**Question**

*For a number field $K$, what possible degrees arise as the degree of a $K$-rational cyclic isogeny between elliptic curves over $K$?*

Let's call this set of possible degrees $\mathrm{IsogCyclicDeg}(K)$.

We write $\mathrm{IsogPrimeDeg}(K)$ for the primes in this set, and call them isogeny primes for $K$.

*A priori* these could be infinite sets.

# The Theorems of Mazur and Kenku

Barry C. Mazur

Monsur A. Kenku

# The Theorems of Mazur and Kenku

**Theorem (Mazur, 1978)**

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

Barry C. Mazur

Monsur A. Kenku

# The Theorems of Mazur and Kenku

**Theorem (Mazur, 1978)**

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

**Theorem (Kenku, 1982)**

$$\text{IsogCyclicDeg}(\mathbb{Q}) = \{1 \quad N \quad 19 \mid \{21, 25, 27, 37, 43, 67, 163\}.$$

Barry C. Mazur

Monsur A. Kenku

# Beyond Mazur's Theorem

# Beyond Mazur's Theorem

**Question**

*Can one write down* $\mathsf{IsogPrimeDeg}(K)$ *for any other number field* $K$*?*

# Beyond Mazur's Theorem

**Question**

*Can one write down* $\mathsf{IsogPrimeDeg}(K)$ *for any other number field* $K$*?*

**Theorem (B., 2021)**

*Assuming GRH, we have the following.*

$$\mathsf{IsogPrimeDeg}(\mathbb{Q}(\sqrt[p]{7})) = \mathsf{IsogPrimeDeg}(\mathbb{Q})$$
$$\mathsf{IsogPrimeDeg}(\mathbb{Q}(\sqrt[p]{10})) = \mathsf{IsogPrimeDeg}(\mathbb{Q})$$
$$\mathsf{IsogPrimeDeg}(\mathbb{Q}(\sqrt[p]{5})) = \mathsf{IsogPrimeDeg}(\mathbb{Q}) \ [\ f23; 47g$$

# Algorithm for Quadratic Isogeny Primes

Actually this is a corollary of the following.

# Algorithm for Quadratic Isogeny Primes

Actually this is a corollary of the following.

## Algorithm (B., 2021)

*Let $K$ be a quadratic field which is not imaginary quadratic of class number 1. Then there is an algorithm which computes a superset of* $\mathrm{IsogPrimeDeg}(K)^*$ *as the union of three sets:*

(*: With these assumptions, this is a finite set, as explained in next section)

# Algorithm for Quadratic Isogeny Primes

Actually this is a corollary of the following.

## Algorithm (B., 2021)

*Let $K$ be a quadratic field which is not imaginary quadratic of class number 1. Then there is an algorithm which computes a superset of* $\mathrm{IsogPrimeDeg}(K)^*$ *as the union of three sets:*

$$\mathrm{IsogPrimeDeg}(K) \quad \mathrm{PreTypeOneTwoPrimes}(K) \; [ \; \mathrm{TypeOnePrimes}(K) \; [ \; \mathrm{TypeTwoPrimes}(K):$$

(*: With these assumptions, this is a finite set, as explained in next section)

# Algorithm for Quadratic Isogeny Primes

Actually this is a corollary of the following.

## Algorithm (B., 2021)

*Let $K$ be a quadratic field which is not imaginary quadratic of class number 1. Then there is an algorithm which computes a superset of* $\mathrm{IsogPrimeDeg}(K)^*$ *as the union of three sets:*

$$\mathrm{IsogPrimeDeg}(K) \quad \mathrm{PreTypeOneTwoPrimes}(K) \; [ \; \mathrm{TypeOnePrimes}(K) \; [ \; \mathrm{TypeTwoPrimes}(K):$$

(*: With these assumptions, this is a finite set, as explained in next section)

## Remark

*If $K$ is imaginary quadratic of class number one, then* $\mathrm{IsogPrimeDeg}(K)$ *is infinite because of complex multiplication.*

# Preview of the Main Calling Function

# Preview of the Main Calling Function

Sage implementation available at

github.com/barinderbanwait/quadratic_isogeny_primes

# Preview of the Main Calling Function

Sage implementation available at

github.com/barinderbanwait/quadratic_isogeny_primes

We'll have a live-demo of the command-line tool after giving an overview of the algorithm.

# PreTypeOneTwoPrimes

# The isogeny character

# The isogeny character

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

# The isogeny character

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

# The isogeny character

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

$$: G_K \to \mathrm{Aut}_V(\overline{K}) = F_p^*;$$

# The isogeny character

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

$$: G_K \to \mathrm{Aut}_V(\overline{K}) = F_p^*;$$

where $V$ is the kernel of the isogeny

# The isogeny character

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

$$: G_K \to \mathrm{Aut}_V(\overline{K}) = F_p^*;$$

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

# The isogeny character

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

$$: G_K \to \mathrm{Aut}_V(\overline{K}) = \mathbb{F}_p^*;$$

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

In 1993, Momose classified isogenies into three types.

# Momose's Classi cation of Isogenies into three types

## Theorem (Momose)

Let $K$ be a number eld. 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 falls into one of the following three types:

# Momose's Classi cation of Isogenies into three types

## Theorem (Momose)

Let $K$ be a number eld. 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 falls into one of the following three types:

Type 1. $^{12}$ or $(\ _p\ ^1)^{12}$ is unrami ed ($_p$ = mod-$p$ cyclotomic character).

# Momose's Classi cation of Isogenies into three types

## Theorem (Momose)

Let $K$ be a number field. 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 falls into one of the following three types:

Type 1. $^{12}$ or $(\ _p\ ^1)^{12}$ is unrami ed ($_p$ = mod-$p$ cyclotomic character).

Type 2. $^{12} = \ ^6_p$ and $p \quad 3 \pmod 4$.

# Momose's Classi cation of Isogenies into three types

## Theorem (Momose)

Let $K$ be a number eld. 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 falls into one of the following three types:

Type 1. $^{12}$ or $(\ _p\ ^1)^{12}$ is unrami ed ($_p$ = mod-$p$ cyclotomic character).

Type 2. $^{12} = \ ^6_p$ and $p \quad 3 \pmod 4$.

Type 3. $K$ contains the Hilbert class eld $H_L$ of an imaginary quadratic eld $L$.

# Momose's Classi cation of Isogenies into three types

## Theorem (Momose)

Let $K$ be a number eld. 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 falls into one of the following three types:

Type 1. $^{12}$ or $(\ _p\ ^1)^{12}$ is unrami ed ($_p$ = mod-$p$ cyclotomic character).

Type 2. $^{12} = \ ^6_p$ and $p \quad 3 \pmod 4$.

Type 3. $K$ contains the Hilbert class eld $H_L$ of an imaginary quadratic eld $L$. The rational prime $p$ splits in $L$:

$$pO_L = pp:$$

# Momose's Classi cation of Isogenies into three types

## Theorem (Momose)

Let $K$ be a number eld. 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 falls into one of the following three types:

Type 1. $^{12}$ or $(\ _p\ ^1)^{12}$ is unrami ed ($_p$ = mod-$p$ cyclotomic character).

Type 2. $^{12} = \ ^6_p$ and $p \quad 3 \pmod 4$.

Type 3. $K$ contains the Hilbert class eld $H_L$ of an imaginary quadratic eld $L$. The rational prime $p$ splits in $L$:

$$pO_L = pp:$$

For any prime $q$ of $K$ prime to $p$,

$$^{12}(\mathrm{Frob}_q) = \ ^{12} \pmod p$$

for any $\ 2 K$ with $O_L = \mathrm{Nm}_{K=L}(q)$.

# PreTypeOneTwoPrimes

Fumiyuki Momose

# PreTypeOneTwoPrimes

## Slogan

If $K$ is a quadratic field which is not imaginary quadratic of class number one, then there is a finite set of primes $\mathrm{PreTypeOneTwoPrimes}(K)$ outside of which the isogeny character is of Type 1 or 2.

# PreTypeOneTwoPrimes

## Slogan

If $K$ is a quadratic field which is not imaginary quadratic of class number one, then there is a finite set of primes $\mathrm{PreTypeOneTwoPrimes}(K)$ outside of which the isogeny character is of Type 1 or 2.

From Momose's Theorem, we could take

$$\mathrm{PreTypeOneTwoPrimes}(K) = \{ p \text{ prime} : p < C_0 \};$$

# PreTypeOneTwoPrimes

## Slogan

If $K$ is a quadratic field which is not imaginary quadratic of class number one, then there is a finite set of primes $\mathrm{PreTypeOneTwoPrimes}(K)$ outside of which the isogeny character is of Type 1 or 2.

From Momose's Theorem, we could take

$$\mathrm{PreTypeOneTwoPrimes}(K) = \{p \text{ prime} : p < C_0\};$$

but we show that it's possible to take the primes dividing a handful of explicitly computable integers.

# PreTypeOneTwoPrimes

## Slogan

If $K$ is a quadratic field which is not imaginary quadratic of class number one, then there is a finite set of primes $\mathrm{PreTypeOneTwoPrimes}(K)$ outside of which the isogeny character is of Type 1 or 2.

From Momose's Theorem, we could take

$$\mathrm{PreTypeOneTwoPrimes}(K) = \{p \text{ prime} : p < C_0\};$$

but we show that it's possible to take the primes dividing a handful of explicitly computable integers.

## Theorem (Momose, Theorem B)

Let $K$ be a quadratic field which is not an imaginary quadratic field of class number 1. Then $\mathrm{IsogPrimeDeg}(K)$ is finite.

# PreTypeOneTwoPrimes

## Slogan

If $K$ is a quadratic field which is not imaginary quadratic of class number one, then there is a finite set of primes $\mathrm{PreTypeOneTwoPrimes}(K)$ outside of which the isogeny character is of Type 1 or 2.

From Momose's Theorem, we could take

$$\mathrm{PreTypeOneTwoPrimes}(K) = \{p \text{ prime} : p < C_0\};$$

but we show that it's possible to take the primes dividing a handful of explicitly computable integers.

## Theorem (Momose, Theorem B)

Let $K$ be a quadratic field which is not an imaginary quadratic field of class number 1. Then $\mathrm{IsogPrimeDeg}(K)$ is finite.

Henceforth, when we say an isogeny-finite $K$, we will mean $K$ as above.

Fumiyuki Momose

# Drilling into Momose's proof I - Finitely many s

By class field theory, we can identify $\chi$ as a character of $I_K(p)$, ideals of $K$ coprime to $p$.

# Drilling into Momose's proof I - Finitely many s

By class field theory, we can identify $\chi$ as a character of $I_K(p)$, ideals of $K$ coprime to $p$.

# Drilling into Momose's proof I - Finitely many s

By class field theory, we can identify $\mathfrak{a}$ as a character of $\mathrm{Cl}_K(p)$, ideals of $K$ coprime to $p$.

For quadratic $K$, we can identify $\mathfrak{a}$ as a pair $(a, b) := a + b\sqrt{\Delta}$, for $\sqrt{\Delta}$ the non-trivial Galois element.

# Drilling into Momose's proof I - Finitely many s

By class field theory, we can identify $\mathfrak{a}$ as a character of $\mathrm{Cl}_K(p)$, ideals of $K$ coprime to $p$.

For quadratic $K$, we can identify $\mathfrak{a}$ as a pair $(a, b) := a + b\sqrt{\Delta}$, for $\sqrt{\Delta}$ the non-trivial Galois element.

Note that the three pairs $(0;0);(12;12);(6;6)$ are not declared here, because ...

# Momose's Classi cation of Isogenies into three types

## Theorem (Momose)

Let $K$ be a number eld. Then there exists an e ective 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 characterfalls into one of the following three types:

Type 1. $^{12}$ or $(\ _p\ ^1)^{12}$ is unrami ed.

Type 2. $^{12} = \ ^6_p$ and $p \quad 3 \pmod 4$.

Type 3. $K$ contains the Hilbert class eld $H_L$ of an imaginary quadratic eld. The rational prime $p$ splits in $L$:

$$pO_L = pp:$$

For any prime $q$ of $K$ prime to $p$,

$$^{12}(\mathrm{Frob}_q) = \ ^{12} \pmod p$$

for any $\ 2\ K$ with $O_L = \mathrm{Nm}_{k=L}(q)$.

# Momose's Classi cation of Isogenies into three types

## Theorem (Momose)

Let $K$ be a number eld. Then there exists an e ective 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 characterfalls into one of the following three types:

Type 1. $^{12}$ or $(\ _p\ ^1)^{12}$ is unrami ed. ( = ( 0; 0) or (12; 12)

Type 2. $^{12} = \ ^6_p$ and $p \quad 3 \pmod 4$. ( = ( 6; 6)

Type 3. $K$ contains the Hilbert class eld $H_L$ of an imaginary quadratic eld. The rational prime $p$ splits in $L$:

$$pO_L = pp:$$

For any prime $q$ of $K$ prime to $p$,

$$^{12}(\mathrm{Frob}_q) = \ ^{12} \pmod p$$

for any $\ 2\ K$ with $O_L = \mathrm{Nm}_{k=L}(q)$.

# Momose's Classi cation of Isogenies into three types

## Theorem (Momose)

Let $K$ be a number eld. Then there exists an e ective 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 characterfalls into one of the following three types:

Type 1. $^{12}$ or $(\ _p\ ^1)^{12}$ is unrami ed. ( = (0;0) or (12;12)

Type 2. $^{12} = \ ^6_p$ and $p \quad 3 \pmod 4$. ( = (6;6)

Type 3. $K$ contains the Hilbert class eld $H_L$ of an imaginary quadratic eld. The rational prime $p$ splits in $L$:

$$pO_L = pp:$$

For any prime $q$ of $K$ prime to $p$,

$$^{12}(\mathrm{Frob}_q) = \ ^{12} \pmod p$$

for any $\ 2\ K$ with $O_L = \mathrm{Nm}_{k=L}(q)$.

# Momose's Classi cation of Isogenies into three types

**Theorem (Momose)**

Let $K$ be a number eld. Then there exists an e ective 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 characterfalls into one of the following three types:

Type 1. $^{12}$ or $(\ _p\ ^1)^{12}$ is unrami ed. ( = ( 0; 0) or (12; 12)

Type 2. $^{12} = \ ^6_p$ and $p \quad 3 \pmod 4$. ( = ( 6; 6)

**To make this explicit ...**

For every other , nd the possible isogeny primes which have an isogeny character acting via .

## Proposition (B.)

If $E$ has a $K$-rational $p$-isogeny with character acting through $\square$, then for all good primes $q$ of $K$, $p$ must divide one of the following:

## Proposition (B.)

If $E$ has a $K$-rational $p$-isogeny with character acting through $\varepsilon$, then for all good* primes $q$ of $K$, $p$ must divide one of the following:

$A(\varepsilon; q) := \mathrm{Nm}_{K/\mathbb{Q}}(\varepsilon - 1)$;

$B(\varepsilon; q) := \mathrm{Nm}_{K/\mathbb{Q}}(\varepsilon - q^{12h_K})$;

$C(\varepsilon; q) := \mathrm{lcm}(\ \mathrm{Nm}_{K(\varepsilon)/\mathbb{Q}}(\varepsilon - \alpha^{12h_K}) \mid \alpha$ is a Frobenius root over $\mathbb{F}_q\ )$:

## Proposition (B.)

If $E$ has a $K$-rational $p$-isogeny with character acting through $\varepsilon$, then for all good* primes $q$ of $K$, $p$ must divide one of the following:

$A(\varepsilon; q) := \mathrm{Nm}_{K/\mathbb{Q}}(\varepsilon - 1)$;

$B(\varepsilon; q) := \mathrm{Nm}_{K/\mathbb{Q}}(\varepsilon - q^{12h_K})$;

$C(\varepsilon; q) := \mathrm{lcm}(\ \mathrm{Nm}_{K(\varepsilon)/\mathbb{Q}}(\varepsilon - \alpha^{12h_K})\ |\ \alpha$ is a Frobenius root over $\mathbb{F}_q\ )$:

(Good means split in $K$, and non-principal if $K$ is imaginary.)

## Proposition (B.)

If $E$ has a $K$-rational $p$-isogeny with character acting through $\varepsilon$, then for all good* primes $q$ of $K$, $p$ must divide one of the following:

$$A(\varepsilon; q) := \mathrm{Nm}_{K/\mathbb{Q}}(\varepsilon - 1);$$

$$B(\varepsilon; q) := \mathrm{Nm}_{K/\mathbb{Q}}(\varepsilon - q^{12h_K});$$

$$C(\varepsilon; q) := \mathrm{lcm}(\ \mathrm{Nm}_{K(\alpha)/\mathbb{Q}}(\alpha^{12h_K} - 1) \mid \alpha \text{ is a Frobenius root over } \mathbb{F}_q\ ):$$

(Good means split in $K$, and non-principal if $K$ is imaginary.)

$$ABC(\varepsilon; q) := \mathrm{Supp}(A(\varepsilon; q)) \cup \mathrm{Supp}(B(\varepsilon; q)) \cup \mathrm{Supp}(C(\varepsilon; q)):$$

## Proposition (B.)

If $E$ has a $K$-rational $p$-isogeny with character acting through $\varepsilon$, then for all good* primes $q$ of $K$, $p$ must divide one of the following:

$$A(\varepsilon; q) := \mathrm{Nm}_{K/\mathbb{Q}}(\varepsilon - 1);$$

$$B(\varepsilon; q) := \mathrm{Nm}_{K/\mathbb{Q}}(\varepsilon - q^{12h_K});$$

$$C(\varepsilon; q) := \mathrm{lcm}(\ \mathrm{Nm}_{K(\alpha)/\mathbb{Q}}(\alpha^{12h_K} - 1) \mid \alpha \text{ is a Frobenius root over } \mathbb{F}_q\ ):$$

(Good means split in $K$, and non-principal if $K$ is imaginary.)

$$ABC(\varepsilon; q) := \mathrm{Supp}(A(\varepsilon; q)) \cup \mathrm{Supp}(B(\varepsilon; q)) \cup \mathrm{Supp}(C(\varepsilon; q)):$$

$$\mathrm{PreTypeOneTwoPrimes}(\varepsilon, K) := \bigcup_{q \in \mathrm{Aux}^2} ABC(\varepsilon; q)$$

## Proposition (B.)

If $E$ has a $K$-rational $p$-isogeny with character acting through $\varepsilon$, then for all good* primes $q$ of $K$, $p$ must divide one of the following:

$$A(\varepsilon; q) := \mathrm{Nm}_{K(\zeta_{12})/\mathbb{Q}}(\varepsilon(\mathrm{Frob}_q) - 1);$$

$$B(\varepsilon; q) := \mathrm{Nm}_{K(\zeta_{12})/\mathbb{Q}}(\varepsilon(\mathrm{Frob}_q) - q^{12h_K});$$

$$C(\varepsilon; q) := \mathrm{lcm}(\ \mathrm{Nm}_{K(\zeta_{12})(\alpha)/\mathbb{Q}}(\alpha^{12h_K} - 1) \mid \alpha \text{ is a Frobenius root over } \mathbb{F}_q\ ):$$

(Good means split in $K$, and non-principal if $K$ is imaginary.)

$$ABC(\varepsilon; q) := \mathrm{Supp}(A(\varepsilon; q)) \cup \mathrm{Supp}(B(\varepsilon; q)) \cup \mathrm{Supp}(C(\varepsilon; q)):$$

$$\mathrm{PreTypeOneTwoPrimes}(\varepsilon, K) := \bigcup_{q \text{ good}} ABC(\varepsilon; q) \setminus \mathrm{Aux}$$

for Aux a finite set of good auxiliary primes.

# A quick glance at the implementation

# TypeTwoPrimes

# Condition CC ...

# Condition CC ...

## Condition CC (Momose + )

Let $K$ be an isogeny- nite quadratic eld, and$E=K$ an elliptic curve admitting a $K$-rational $p$-isogeny, with$p$ of Type 2.

# Condition CC ...

## Condition CC (Momose + )

Let K be an isogeny- nite quadratic eld, and E=K an elliptic curve admitting a K-rational p-isogeny, with p of Type 2. Let q be a rational prime < p=4 such that $q^2 + q + 1 \not\equiv 0 \pmod{p}$. Then the following implication holds:

# Condition CC ...

## Condition CC (Momose + )

Let $K$ be an isogeny- nite quadratic eld, and $E=K$ an elliptic curve admitting a $K$-rational $p$-isogeny, with $p$ of Type 2. Let $q$ be a rational prime $< p=4$ such that $q^2 + q + 1 \not\equiv 0 \pmod{p}$. Then the following implication holds:

if $q$ splits or rami es in $K$, then $q$ does not split in $Q(\sqrt{p})$.

# Condition CC ...

## Condition CC (Momose + )

Let $K$ be an isogeny- nite quadratic eld, and $E=K$ an elliptic curve admitting a $K$-rational $p$-isogeny, with $p$ of Type 2. Let $q$ be a rational prime $< p=4$ such that $q^2 + q + 1 \not\equiv 0 \pmod{p}$. Then the following implication holds:

if $q$ splits or rami es in $K$, then $q$ does not split in $Q(\sqrt{p})$.

# ... Generalises Mazur's Claim

Barry C. Mazur receives National Medal of Science from US President Barack H. Obama

# ... Generalises Mazur's Claim

Barry C. Mazur receives National Medal of Science from US President Barack H. Obama

Determining the Type 2 primes is harder for general $K$.

Determining the Type 2 primes is harder for general $K$.

Larson and Vaintrob obtained a bound on these primes involving "effectively computable absolute constants".

Determining the Type 2 primes is harder for general $K$.
Larson and Vaintrob obtained a bound on these primes involving "effectively computable absolute constants".

Eric Larson Dmitry Vaintrob

Determining the Type 2 primes is harder for general $K$.
Larson and Vaintrob obtained a bound on these primes involving "effectively computable absolute constants".

Eric Larson Dmitry Vaintrob

Determining the Type 2 primes is harder for general $K$.
Larson and Vaintrob obtained a bound on these primes involving "effectively computable absolute constants".

Eric Larson Dmitry Vaintrob

**Question**

Can we remove the "effectively computable absolute constants"?

## Proposition (B.)

Assume GRH. Let $K$ be an isogeny-finite quadratic field, and $E/K$ an elliptic curve possessing a $K$-rational $p$-isogeny, for $p$ a Type 2 prime. Then $p$ satisfies

$$p \leq (16 \log p + 16 \log(12 \Delta_K) + 26)^4.$$

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

## Proposition (B.)

Assume GRH. Let $K$ be an isogeny-finite quadratic field, and $E/K$ an elliptic curve possessing a $K$-rational $p$-isogeny, for $p$ a Type 2 prime. Then $p$ satisfies

$$p \quad (16 \log p + 16 \log(12 \quad _K) + 26)^4 :$$

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

## Strategy

Check all primes up to this bound for whether they satisfy condition CC or not.

# Live Demo

$$\mathrm{IsogPrimeDeg}(\mathbb{Q}(\sqrt{5}))$$

To determine:

$$\{23, 29, 31, 41, 47, 53, 59, 61, 71, 73, 79\}:$$

To determine:

$$\{23, 29, 31, 41, 47, 53, 59, 61, 71, 73, 79\}:$$

i.e. for each $p$ in this set, determine whether the modular curve $X_0(p)$ admits any non-cuspidal $\mathbb{Q}(\sqrt{5})$-rational points.

To determine:

$$\{23, 29, 31, 41, 47, 53, 59, 61, 71, 73, 79\}:$$

i.e. for each $p$ in this set, determine whether the modular curve $X_0(p)$ admits any non-cuspidal $\mathbb{Q}(\sqrt{-5})$-rational points.

$X_0(23)$ does admit such points:

To determine:

$$\{23, 29, 31, 41, 47, 53, 59, 61, 71, 73, 79\}:$$

i.e. for each $p$ in this set, determine whether the modular curve $X_0(p)$ admits any non-cuspidal $\mathbb{Q}(\sqrt{-5})$-rational points.

$X_0(23)$ does admit such points:

To determine:

$$\{23, 29, 31, 41, 47, 53, 59, 61, 71, 73, 79\}:$$

i.e. for each $p$ in this set, determine whether the modular curve $X_0(p)$ admits any non-cuspidal $\mathbb{Q}(\sqrt{5})$-rational points.

$X_0(23)$ does admit such points:

This method also works for 47.

To determine:

$$\{23, 29, 31, 41, 47, 53, 59, 61, 71, 73, 79\}:$$

i.e. for each $p$ in this set, determine whether the modular curve $X_0(p)$ admits any non-cuspidal $\mathbb{Q}(\sqrt{-5})$-rational points.

$X_0(23)$ does admit such points:

This method also works for 47. But it doesn't work for the other cases.

To determine:

$$\{23, 29, 31, 41, 47, 53, 59, 61, 71, 73, 79\}:$$

i.e. for each $p$ in this set, determine whether the modular curve $X_0(p)$ admits any non-cuspidal $\mathbb{Q}(\sqrt{-5})$-rational points.

$X_0(23)$ does admit such points:

This method also works for 47. But it doesn't work for the other cases.

All of these primes are such that genus$(X_0(p)) \geq 5$.

# Quadratic Points of Low-genus modular curves

Hyperelliptic modular curves $X_0(N)$ and isogenies of elliptic curves over quadratic fields, 2015

Peter J. Bruin

Filip Najman

Quadratic points on modular curves, 2019

Ekin Özman

Samir Siksek

Quadratic points on modular curves with infinite Mordell-Weil group, 2021

Josha Box

# Summary

Using their results, we can rule out the other values to conclude that

$$\text{IsogPrimeDeg}(\mathbb{Q}(\sqrt{5})) = \text{IsogPrimeDeg}(\mathbb{Q}) \setminus \{23, 47\}.$$

# Summary

Using their results, we can rule out the other values to conclude that

$$\mathrm{IsogPrimeDeg}_{\mathbb{Q}(\sqrt{5})}(\mathbb{Q}(\sqrt{5})) = \mathrm{IsogPrimeDeg}_{\mathbb{Q}}(\mathbb{Q}) \cap \{2, 3, 23, 47\}.$$

One similarly shows

$$\mathrm{IsogPrimeDeg}_{\mathbb{Q}(\sqrt{7})}(\mathbb{Q}(\sqrt{7})) = \mathrm{IsogPrimeDeg}_{\mathbb{Q}}(\mathbb{Q}).$$
$$\mathrm{IsogPrimeDeg}_{\mathbb{Q}(\sqrt{-10})}(\mathbb{Q}(\sqrt{-10})) = \mathrm{IsogPrimeDeg}_{\mathbb{Q}}(\mathbb{Q}).$$

# Summary

Using their results, we can rule out the other values to conclude that

$$\mathrm{IsogPrimeDeg}_{\mathbb{Q}(\sqrt{5})}(\mathbb{Q}(\sqrt{5})) = \mathrm{IsogPrimeDeg}_{\mathbb{Q}}(\mathbb{Q}) \cup \{23, 47\}.$$

One similarly shows

$$\mathrm{IsogPrimeDeg}_{\mathbb{Q}(\sqrt{7})}(\mathbb{Q}(\sqrt{7})) = \mathrm{IsogPrimeDeg}_{\mathbb{Q}}(\mathbb{Q}).$$
$$\mathrm{IsogPrimeDeg}_{\mathbb{Q}(\sqrt{10})}(\mathbb{Q}(\sqrt{10})) = \mathrm{IsogPrimeDeg}_{\mathbb{Q}}(\mathbb{Q}).$$

See the final section of the paper for the details.

# Further Avenues

Working on determining IsogCyclicDeg(K) for certain K's with Oana Adascalitei in Boston, USA, and Filip Najman in Zagreb, Croatia.

Working on determining IsogCyclicDeg($\mathcal{O}$K) for certain K's with Oana Adascalitei in Boston, USA, and Filip Najman in Zagreb, Croatia.

Working on extending the methods to cubic and higher degree number fields with Maarten Derickx in Den Haag, The Netherlands.

Working on determining IsogCyclicDeg($K$) for certain $K$s with Oana Adascalitei in Boston, USA, and Filip Najman in Zagreb, Croatia.

Working on extending the methods to cubic and higher degree number fields with Maarten Derickx in Den Haag, The Netherlands.

I'll be giving a live demo of our latest algorithm on a cubic field at my VaNTAGe seminar talk on June 29th: `https://sites.google.com/view/vantageseminar`

# Thanks for listening!

| Image | Copyright Holder | License |
|---|---|---|
|  | George M. Bergman, via MFO | CC BY-SA 2.0 |
|  | George M. Bergman, via MFO | CC BY-SA 2.0 |
| | Ada Goldfeld | Written permission obtained |
| | Univ. of Washington | Fair use |
| | Peter J. Bruin | Fair use |
| | Univ. of Warwick | Fair use |

| Image | Copyright Holder | License |
|---|---|---|
| | Math. Dept., Chuo University, Tokyo, Japan | Fair use |
| | Maarten Derickx | Fair use |
| | Getty images/Jewel Samad | Fair use (embed) |
| | Dmitry Vaintrob | Fair use |
| | Matematički kolokvij u Osijeku | Fair use |
| | Ekin Özman | Fair use |
| | Univ. of Warwick | Fair use |

MFO = Mathematisches Forschungsinstitut Oberwolfach