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 $\phi : E_1 \to E_2$ 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};

$\Leftrightarrow$ 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};

$\Leftrightarrow$ induces a group homomorphism from $E_1(\overline{K})$ to $E_2(\overline{K})$;

$\Leftrightarrow$ 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 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 $\sigma \in G_K$:

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

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

$$\begin{aligned}\{K\text{-rational isogenies from } E\} &\xrightarrow{\sim} \{G_K\text{-invariant finite subgroups of } E(\overline{K})\}\\ \phi &\longmapsto \ker\phi\\ \phi_C : E \to E/C &\longleftarrow\!\shortmid C.\end{aligned}$$

Isogenies = Kernel

Fact

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

$$\begin{aligned}\{K\text{-rational isogenies from } E\} &\xrightarrow{\sim} \{G_K\text{-invariant finite subgroups of } E(\overline{K})\}\\ \phi &\longmapsto \ker\phi\\ \phi_C : E \to E/C &\longleftarrow C.\end{aligned}$$

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 $\text{IsogCyclicDeg}(K)$.

We write $\text{IsogPrimeDeg}(K)$ 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)

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

Barry C. Mazur

Monsur A. Kenku

The Theorems of Mazur and Kenku

Theorem (Mazur, 1978)

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

Theorem (Kenku, 1982)

$$\mathrm{IsogCyclicDeg}(\mathbb{Q}) = \{1 \leq N \leq 19\} \cup \{21, 25, 27, 37, 43, 67, 163\}.$$

Barry C. Mazur

Monsur A. Kenku

Beyond Mazur's Theorem

Beyond Mazur's Theorem

Question

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

Beyond Mazur's Theorem

Question

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

Theorem (B., 2021)

Assuming GRH, we have the following.

$$\mathrm{IsogPrimeDeg}(\mathbb{Q}(\sqrt{7})) = \mathrm{IsogPrimeDeg}(\mathbb{Q})$$
$$\mathrm{IsogPrimeDeg}(\mathbb{Q}(\sqrt{-10})) = \mathrm{IsogPrimeDeg}(\mathbb{Q})$$
$$\mathrm{IsogPrimeDeg}(\mathbb{Q}(\sqrt{5})) = \mathrm{IsogPrimeDeg}(\mathbb{Q}) \cup \{23, 47\}$$

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:*

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

(*: 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:*

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

(*: 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

```python
def get_isogeny_primes(K, aux_prime_count, bound=1000, loop_only_j=True):

    # Start with some helpful user info

    print("\nFinding isogeny primes for {}\n".format(K))
    print("Number of auxiliary primes is {}\n".format(aux_prime_count))

    # Get and show TypeOnePrimes

    type_1_primes = get_type_1_primes(K, aux_prime_count=aux_prime_count,
                                      loop_only_j=loop_only_j)
    print("type_1_primes = {}\n".format(type_1_primes))

    # Get and show PreTypeOneTwoPrimes

    pre_type_one_two_primes = get_pre_type_one_two_primes(K,
                                aux_prime_count=aux_prime_count,
                                loop_only_j=loop_only_j)
    print("pre_type_2_primes = {}\n".format(pre_type_one_two_primes))

    # Get and show TypeTwoPrimes

    type_2_primes = get_type_2_primes(K, bound=bound)
    print("type_2_primes = {}\n".format(type_2_primes))

    # Put them all together and sort the list before returning
    candidates = set.union(set(type_1_primes),
                           set(pre_type_one_two_primes),
                           set(type_2_primes))
    candidates = list(candidates)
    candidates.sort()

    return candidates

```

Preview of the Main Calling Function

Sage implementation available at

`github.com/barinderbanwait/quadratic_isogeny_primes`

```
def get_isogeny_primes(K, aux_prime_count, bound=1000, loop_only_j=True):

    # Start with some helpful user info

    print("\nFinding isogeny primes for {}\n".format(K))
    print("Number of auxiliary primes is {}\n".format(aux_prime_count))

    # Get and show TypeOnePrimes

    type_1_primes = get_type_1_primes(K, aux_prime_count=aux_prime_count,
                                      loop_only_j=loop_only_j)
    print("type_1_primes = {}\n".format(type_1_primes))

    # Get and show PreTypeOneTwoPrimes

    pre_type_one_two_primes = get_pre_type_one_two_primes(K,
                              aux_prime_count=aux_prime_count,
                              loop_only_j=loop_only_j)
    print("pre_type_2_primes = {}\n".format(pre_type_one_two_primes))

    # Get and show TypeTwoPrimes

    type_2_primes = get_type_2_primes(K, bound=bound)
    print("type_2_primes = {}\n".format(type_2_primes))

    # Put them all together and sort the list before returning
    candidates = set.union(set(type_1_primes),
                           set(pre_type_one_two_primes),
                           set(type_2_primes))
    candidates = list(candidates)
    candidates.sort()

    return candidates
```

Preview of the Main Calling Function

Sage implementation available at

github.com/barinderbanwait/quadratic_isogeny_primes

```python
def get_isogeny_primes(K, aux_prime_count, bound=1000, loop_only_j=True):

    # Start with some helpful user info

    print("\nFinding isogeny primes for {}\n".format(K))
    print("Number of auxiliary primes is {}\n".format(aux_prime_count))

    # Get and show TypeOnePrimes

    type_1_primes = get_type_1_primes(K, aux_prime_count=aux_prime_count,
                                      loop_only_j=loop_only_j)
    print("type_1_primes = {}\n".format(type_1_primes))

    # Get and show PreTypeOneTwoPrimes

    pre_type_one_two_primes = get_pre_type_one_two_primes(K,
                                  aux_prime_count=aux_prime_count,
                                  loop_only_j=loop_only_j)
    print("pre_type_2_primes = {}\n".format(pre_type_one_two_primes))

    # Get and show TypeTwoPrimes

    type_2_primes = get_type_2_primes(K, bound=bound)
    print("type_2_primes = {}\n".format(type_2_primes))

    # Put them all together and sort the list before returning
    candidates = set.union(set(type_1_primes),
                           set(pre_type_one_two_primes),
                           set(type_2_primes))
    candidates = list(candidates)
    candidates.sort()

    return candidates
```

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 λ 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 λ denote the isogeny character:

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

The isogeny character

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

The isogeny character

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.

The isogeny character

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.

Isogenies of prime degree over number fields

FUMIYUKI MOMOSE
Department of Mathematics, Chuo University, 1-13-27 Kasuga, Bunkyo-ku, Tokyo 112, Japan

Received 19 August 1993; accepted in final form 24 December 1993

In 1993, Momose classified isogenies into three types.

Momose's Classification 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 λ falls into one of the following three types:

Momose's Classification 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 λ falls into one of the following three types:

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

Momose's Classification 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 λ falls into one of the following three types:

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

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

Momose's Classification 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 λ falls into one of the following three 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* $p \equiv 3 \pmod 4$.

Type 3. K *contains the Hilbert class field* H_L *of an imaginary quadratic field* L.

Momose's Classification 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 λ falls into one of the following three types:

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

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

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

$$p\mathcal{O}_L = \mathfrak{p}\bar{\mathfrak{p}}.$$

Momose's Classification 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 λ falls into one of the following three types:

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

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

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

$$p\mathcal{O}_L = \mathfrak{p}\bar{\mathfrak{p}}.$$

For any prime $\mathfrak{q}$ *of* K *prime to* $\mathfrak{p}$,

$$\lambda^{12}(\mathrm{Frob}_{\mathfrak{q}}) = \alpha^{12} \pmod{\mathfrak{p}}$$

for any $\alpha \in K^\times$ *with* $\alpha\mathcal{O}_L = \mathrm{Nm}_{K/L}(\mathfrak{q})$.

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 PreTypeOneTwoPrimes(K) outside of which the isogeny character is of Type 1 or 2.

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 PreTypeOneTwoPrimes(K) outside of which the isogeny character is of Type 1 or 2.

From Momose's Theorem, we *could* take

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

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 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.

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.

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.

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 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 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 ϵs

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

Drilling into Momose's proof I - Finitely many ϵs

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.

Drilling into Momose's proof I - Finitely many ϵs

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.

For quadratic K, we can identify ϵ as a pair $(a, b) := a + b\sigma$, for σ the non-trivial Galois element.

Drilling into Momose's proof I - Finitely many ϵs

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.

For quadratic K, we can identify ϵ as a pair $(a, b) := a + b\sigma$, for σ the non-trivial Galois element.

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]).

```python
# The PreTypeOneTwo epsilons, with their types
EPSILONS_PRE_TYPE_1_2 = {

    (0,12): 'quadratic',
    (12,0): 'quadratic',

    (0,4): 'quartic',
    (0,8): 'quartic',
    (4,0): 'quartic',
    (4,4): 'quartic',
    (4,8): 'quartic',
    (4,12): 'quartic',
    (8,0): 'quartic',
    (8,4): 'quartic',
    (8,8): 'quartic',
    (8,12): 'quartic',
    (12,4): 'quartic',
    (12,8): 'quartic',

    (0,6) : 'sextic',
    (6,0) : 'sextic',
    (6,12) : 'sextic',
    (12,6) : 'sextic'
}
```

```
# The PreTypeOneTwo epsilons, with their types
EPSILONS_PRE_TYPE_1_2 = {

    (0,12): 'quadratic',
    (12,0): 'quadratic',

    (0,4): 'quartic',
    (0,8): 'quartic',
    (4,0): 'quartic',
    (4,4): 'quartic',
    (4,8): 'quartic',
    (4,12): 'quartic',
    (8,0): 'quartic',
    (8,4): 'quartic',
    (8,8): 'quartic',
    (8,12): 'quartic',
    (12,4): 'quartic',
    (12,8): 'quartic',

    (0,6) : 'sextic',
    (6,0) : 'sextic',
    (6,12) : 'sextic',
    (12,6) : 'sextic'
}
```

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

Momose's Classification of Isogenies into three types

Theorem (Momose)

Let K be a number field. Then there exists an effective 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 three types:

Type 1. λ^{12} *or* $(\lambda\theta_p^{-1})^{12}$ *is unramified.*

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

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

$$p\mathcal{O}_L = \mathfrak{p}\bar{\mathfrak{p}}.$$

For any prime $\mathfrak{q}$ *of* K *prime to* $\mathfrak{p}$,

$$\lambda^{12}(\mathrm{Frob}_{\mathfrak{q}}) = \alpha^{12} \pmod{\mathfrak{p}}$$

for any $\alpha \in K^\times$ *with* $\alpha\mathcal{O}_L = \mathrm{Nm}_{k/L}(\mathfrak{q})$.

Momose's Classification of Isogenies into three types

Theorem (Momose)

Let K be a number field. Then there exists an effective 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 three types:

Type 1. λ^{12} *or* $(\lambda\theta_p^{-1})^{12}$ *is unramified.* $\Leftarrow \epsilon = (0,0)$ *or* $(12,12)$

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

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

$$p\mathcal{O}_L = \mathfrak{p}\bar{\mathfrak{p}}.$$

For any prime $\mathfrak{q}$ of K prime to $\mathfrak{p}$,

$$\lambda^{12}(\mathrm{Frob}_{\mathfrak{q}}) = \alpha^{12} \pmod{\mathfrak{p}}$$

for any $\alpha \in K^\times$ with $\alpha\mathcal{O}_L = \mathrm{Nm}_{k/L}(\mathfrak{q})$.

Momose's Classification of Isogenies into three types

Theorem (Momose)

Let K be a number field. Then there exists an effective 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 three types:

Type 1. λ^{12} *or* $(\lambda\theta_p^{-1})^{12}$ *is unramified.* $\Leftarrow \epsilon = (0,0)$ *or* $(12,12)$

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

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

$$p\mathcal{O}_L = \mathfrak{p}\bar{\mathfrak{p}}.$$

For any prime $\mathfrak{q}$ of K prime to $\mathfrak{p}$,

$$\lambda^{12}(\mathrm{Frob}_\mathfrak{q}) = \alpha^{12} \pmod{\mathfrak{p}}$$

for any $\alpha \in K^\times$ with $\alpha\mathcal{O}_L = \mathrm{Nm}_{k/L}(\mathfrak{q})$.

Momose's Classification of Isogenies into three types

Theorem (Momose)

Let K be a number field. Then there exists an effective 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 three types:

Type 1. λ^{12} *or* $(\lambda\theta_p^{-1})^{12}$ *is unramified.* $\Leftarrow \epsilon = (0,0)$ *or* $(12,12)$

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

To make this explicit ...

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

Proposition (B.)

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

Proposition (B.)

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

$$A(\epsilon, \mathfrak{q}) := \mathrm{Nm}_{K/\mathbb{Q}}(\alpha^{\epsilon} - 1);$$

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

$$C(\epsilon, \mathfrak{q}) := \mathrm{lcm}(\{\mathrm{Nm}_{K(\beta)/\mathbb{Q}}(\alpha^{\epsilon} - \beta^{12h_K}) \mid \beta \text{ is a Frobenius root over } \mathbb{F}_{\mathfrak{q}}\}).$$

Proposition (B.)

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

$$A(\epsilon, \mathfrak{q}) := \mathrm{Nm}_{K/\mathbb{Q}}(\alpha^{\epsilon} - 1);$$

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

$$C(\epsilon, \mathfrak{q}) := \mathrm{lcm}(\{\mathrm{Nm}_{K(\beta)/\mathbb{Q}}(\alpha^{\epsilon} - \beta^{12h_K}) \mid \beta \text{ is a Frobenius root over } \mathbb{F}_{\mathfrak{q}}\}).$$

(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 ϵ, then for all good primes $\mathfrak{q}$ of K, p must divide one of the following:*

$$A(\epsilon, \mathfrak{q}) := \mathrm{Nm}_{K/\mathbb{Q}}(\alpha^{\epsilon} - 1);$$

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

$$C(\epsilon, \mathfrak{q}) := \mathrm{lcm}(\{\mathrm{Nm}_{K(\beta)/\mathbb{Q}}(\alpha^{\epsilon} - \beta^{12h_K}) \mid \beta \textit{ is a Frobenius root over } \mathbb{F}_{\mathfrak{q}}\}).$$

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

$$ABC(\epsilon, \mathfrak{q}) := \mathrm{Supp}(A(\epsilon, \mathfrak{q})) \cup \mathrm{Supp}(B(\epsilon, \mathfrak{q})) \cup \mathrm{Supp}(C(\epsilon, \mathfrak{q})).$$

Proposition (B.)

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

$$A(\epsilon, \mathfrak{q}) := \mathrm{Nm}_{K/\mathbb{Q}}(\alpha^{\epsilon} - 1);$$

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

$$C(\epsilon, \mathfrak{q}) := \mathrm{lcm}(\{\mathrm{Nm}_{K(\beta)/\mathbb{Q}}(\alpha^{\epsilon} - \beta^{12h_K}) \mid \beta \textit{ is a Frobenius root over } \mathbb{F}_{\mathfrak{q}}\}).$$

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

$$ABC(\epsilon, \mathfrak{q}) := \mathrm{Supp}(A(\epsilon, \mathfrak{q})) \cup \mathrm{Supp}(B(\epsilon, \mathfrak{q})) \cup \mathrm{Supp}(C(\epsilon, \mathfrak{q})).$$

$$\mathrm{PreTypeOneTwoPrimes}(K) := \bigcup_{\epsilon} \bigcap_{\mathfrak{q} \in \mathrm{Aux}} ABC(\epsilon, \mathfrak{q})$$

Proposition (B.)

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

$$A(\epsilon, \mathfrak{q}) := \mathrm{Nm}_{K/\mathbb{Q}}(\alpha^\epsilon - 1);$$
$$B(\epsilon, \mathfrak{q}) := \mathrm{Nm}_{K/\mathbb{Q}}(\alpha^\epsilon - q^{12h_K});$$
$$C(\epsilon, \mathfrak{q}) := \mathrm{lcm}(\{\mathrm{Nm}_{K(\beta)/\mathbb{Q}}(\alpha^\epsilon - \beta^{12h_K}) \mid \beta \text{ is a Frobenius root over } \mathbb{F}_\mathfrak{q}\}).$$

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

$$ABC(\epsilon, \mathfrak{q}) := \mathrm{Supp}(A(\epsilon, \mathfrak{q})) \cup \mathrm{Supp}(B(\epsilon, \mathfrak{q})) \cup \mathrm{Supp}(C(\epsilon, \mathfrak{q})).$$

$$\mathrm{PreTypeOneTwoPrimes}(K) := \bigcup_{\epsilon} \bigcap_{\mathfrak{q} \in \mathrm{Aux}} ABC(\epsilon, \mathfrak{q})$$

for Aux a finite set of good **auxiliary primes**.

A quick glance at the implementation

```
def get_AB_primes(K, q, epsilons, q_class_group_order):

    output_dict_AB = {}
    alphas = (q ** q_class_group_order).gens_reduced()
    assert len(alphas) == 1, "q^q_class_group_order not principal, which is very bad"
    alpha = alphas[0]
    rat_q = ZZ(q.norm())
    assert rat_q.is_prime(), "somehow the degree 1 prime is not prime"
    for eps in epsilons:
        alpha_to_eps = group_ring_exp(alpha,eps)
        A = (alpha_to_eps - 1).norm()
        B = (alpha_to_eps - (rat_q ** (12 * q_class_group_order))).norm()
        output_dict_AB[eps] = lcm(A,B)
    return output_dict_AB
```

```
for frob_poly in frob_polys_to_loop:
    if frob_poly.is_irreducible():
        frob_poly_root_field = frob_poly.root_field('a')
        _, K_into_KL, L_into_KL, _ = K.composite_fields(frob_poly_root_field, 'c', bot
    else:
        frob_poly_root_field = IntegerRing()
    roots_of_frob = frob_poly.roots(frob_poly_root_field)
    betas = [r for r,e in roots_of_frob]

    for beta in betas:
        if beta in K:
            for eps in epsilons:
                N = (group_ring_exp(alpha, eps) - beta ** (12*q_class_group_order)).ab
                N = ZZ(N)
                output_dict_C[eps] = lcm(output_dict_C[eps], N)
        else:
            for eps in epsilons:
                N = (K_into_KL(group_ring_exp(alpha, eps)) - L_into_KL(beta ** (12*q_c
                N = ZZ(N)
                output_dict_C[eps] = lcm(output_dict_C[eps], N)
return output_dict_C
```

TypeTwoPrimes

Condition CC ...

Condition CC ...

Condition CC (Momose + ϵ)

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

Condition CC ...

Condition CC (Momose + ϵ)

Let K be an isogeny-finite quadratic field, 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 + ϵ)

Let K be an isogeny-finite quadratic field, 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 ramifies in K, then q does not split in $\mathbb{Q}(\sqrt{-p})$.

Condition CC ...

Condition CC (Momose + ϵ)

Let K be an isogeny-finite quadratic field, 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:

$$\text{if } q \text{ splits or ramifies in } K, \text{ then } q \text{ does not split in } \mathbb{Q}(\sqrt{-p}).$$

Dorian Goldfeld

Appendix. *An Analogue of the Class Number One Problem*

By D. Goldfeld

1. Let K be an algebraic number field of finite degree over $\mathbf{Q}$ with discriminant k, and let S be a finite set of rational primes. Define $\mathcal{N}(K, S)$ to be the set of rational integers N satisfying the conditions:

$-N$ is a discriminant of a quadratic field and for all primes $l \notin S$, $l < |N|/4$, if l splits completely in K, then l doesn't split in $\mathbf{Q}(\sqrt{-N})$.

In the case that K is equal to $\mathbf{Q}$ or a quadratic field, we shall show that $\mathcal{N}(K, S)$ is a finite set. The method of proof, however, is ineffective and all that can be deduced is

… Generalises Mazur's Claim

Claim. If the above case occurs then for all odd primes $p < N/4$ *we have* $\left(\frac{p}{N}\right) = -1$.

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

… Generalises Mazur's Claim

Claim. If the above case occurs then for all odd primes $p < N/4$ we have $\left(\frac{p}{N}\right) = -1$.

To conclude our theorem, we shall now prove that the above *claim* implies that $\mathbf{Q}(\sqrt{-N})$ has class number 1 and hence (by Baker-Stark-Heegner [3, 37, 38]) we have $N = 11, 19, 43, 67$, or 163 (ignoring the genus 0 cases).

Since $N \equiv -1 \bmod 4$, quadratic reciprocity applied to (7.1) implies that for $2 < p < N/4$, p remains prime in $\mathbf{Q}(\sqrt{-N})$.

Thus all ideals I of odd norm $< N/4$ are principal in the ring of integers of $\mathbf{Q}(\sqrt{-N})$. To be sure, if we had the stronger assertion that *all* ideals of norm $< N/4$ were principal, then $\mathbf{Q}(\sqrt{-N})$ would have class number 1 by Minkowski's theorem: the absolute value of the discriminant of $\mathbf{Q}(\sqrt{-N})$ is N; the Minkowski constant is $2/\pi$; and $2/\pi \cdot \sqrt{N} < N/4$ for $N \geqq 11$. We shall prove this stronger assertion. If 2 does not split in $\mathbf{Q}(\sqrt{-N})$, there is nothing to prove. Suppose, then, that 2 does split, in which case $N \equiv -1$ or $7 \bmod 16$. We must show that one (and hence both) of the primes of norm 2 are principal. If $N \equiv -1 \bmod 16$, consider the element $\alpha = (3 + \sqrt{-N})/2$. One sees that the norm of α is twice an odd number; hence $(\alpha) = \mathfrak{p} \cdot I$ where $\mathfrak{p}$ is one of the primes of norm 2, and I is an "odd" ideal, with norm $(9 + N)/8$. Since $N \geqq 11$, the norm of I is less than $N/4$, and therefore I is principal. Consequently so is $\mathfrak{p}$. If $N \equiv 7 \bmod 16$, take the element $\alpha = (1 + \sqrt{-N})/2$, and repeat the above argument.

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

Theorem 7.9. *Under GRH, there are effectively computable absolute constants c_2, c_3, and c_4 such that we can take in Theorems 6.4 and 5.16*

$$\prod_{\ell \in S_K} \ell \leqslant \exp\left(c_2^{n_K} \cdot \left(R_K \cdot n_K^{r_K} + h_K^2 \cdot (\log \Delta_K)^2\right)\right)$$

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

Theorem 7.9. *Under GRH, there are effectively computable absolute constants c_2, c_3, and c_4 such that we can take in Theorems 6.4 and 5.16*

$$\prod_{\ell \in S_K} \ell \leqslant \exp\left(c_2^{n_K} \cdot \left(R_K \cdot n_K^{r_K} + h_K^2 \cdot (\log \Delta_K)^2\right)\right)$$

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

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

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.

```python
def get_type_2_primes(K, bound=None):
    """Compute a list containing the type 2 primes"""

    # First get the bound
    if bound is None:
        bound = get_type_2_bound(K)
        print("type 2 bound = {}".format(bound))

    # We need to include all primes up to 25
    # see Larson/Vaintrob's proof of Theorem 6.4
    output = set(prime_range(25))

    for p in pari.primes(25, bound):
        p_int = Integer(p)
        if p_int % 4 == 3:  # Type 2 primes necessarily congruent to 3 mod 4
            if satisfies_condition_CC(K,p_int):
                output.add(p_int)
    return output
```

```
blockSize=100000;
export(blockSize)

checktypetwo(pBeg) =
{
    my(p,cond);
    forprime(p = pBeg*blockSize, (pBeg+1)*blockSize-1,
        cond=custom_congruence_condition(p,D);
        if(cond,print_satisfiesCC(p)));
}
export(checktypetwo)

howMany=floor(typetwobound/blockSize);
parapply(checktypetwo,[0..howMany]);
```

Live Demo

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:

MAGMA
COMPUTER • ALGEBRA

```
Type ? for help.  Type <Ctrl>-D to quit.
> R<x> := PolynomialRing(Rationals());
> K<a> := NumberField(R![-1, -1, 1]);
> N:=23;
> X := SmallModularCurve(N,K);
> RationalPoints(X : Bound:=10);
{@ (1 : 0 : 0), (1 : 1 : 0), (-3 : 23*a - 26 : 1), (-3 : -23*a - 3 : 1) @}
```

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:

MAGMA
COMPUTER • ALGEBRA

```
Type ? for help.  Type <Ctrl>-D to quit.
> R<x> := PolynomialRing(Rationals());
> K<a> := NumberField(R![-1, -1, 1]);
> N:=23;
> X := SmallModularCurve(N,K);
> RationalPoints(X : Bound:=10);
{@ (1 : 0 : 0), (1 : 1 : 0), (-3 : 23*a - 26 : 1), (-3 : -23*a - 3 : 1) @}
```

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:

MAGMA COMPUTER • ALGEBRA

```
Type ? for help.  Type <Ctrl>-D to quit.
> R<x> := PolynomialRing(Rationals());
> K<a> := NumberField(R![-1, -1, 1]);
> N:=23;
> X := SmallModularCurve(N,K);
> RationalPoints(X : Bound:=10);
{@ (1 : 0 : 0), (1 : 1 : 0), (-3 : 23*a - 26 : 1), (-3 : -23*a - 3 : 1) @}
```

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:

MAGMA
COMPUTER • ALGEBRA

```
Type ? for help.  Type <Ctrl>-D to quit.
> R<x> := PolynomialRing(Rationals());
> K<a> := NumberField(R![-1, -1, 1]);
> N:=23;
> X := SmallModularCurve(N,K);
> RationalPoints(X : Bound:=10);
{@ (1 : 0 : 0), (1 : 1 : 0), (-3 : 23*a - 26 : 1), (-3 : -23*a - 3 : 1) @}
```

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

All of these primes are such that $\mathrm{genus}(X_0(p)) \leq 5$.

Quadratic Points of Low-genus modular curves

Peter J. Bruin

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

Filip Najman

Ekin Özman

Quadratic points on modular curves, 2019

Samir Siksek

Josha Box

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

Summary

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

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

Summary

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

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

One similarly shows

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

Summary

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

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

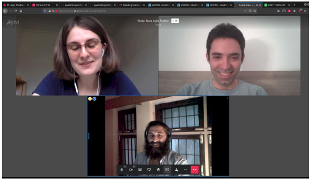
One similarly shows

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

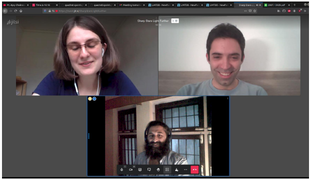
See the final section of the paper for the details.

Further Avenues

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

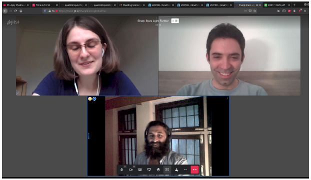


Working on determining IsogCyclicDeg(K) for certain Ks with Oana Adascalitei in Boston, USA, and Filip Najman in Zagreb, Croatia.



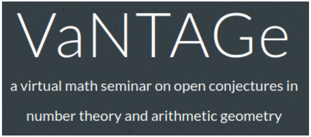
Working on extending the methods to cubic and higher degree number fields with Maarten Derickx in Den Haag, The Netherlands.

Working on determining IsogCyclicDeg(K) for certain Ks 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	Image	Copyright Holder	License
	George M. Bergman, via MFO	CC BY-SA 2.0		Math. Dept., Chuo University, Tokyo, Japan	Fair use
	George M. Bergman, via MFO	CC BY-SA 2.0		Maarten Derickx	Fair use
	Ada Goldfeld	Written permission obtained		Getty images/Jewel Samad	Fair use (embed)
	Univ. of Washington	Fair use		Dmitry Vaintrob	Fair use
	Peter J. Bruin	Fair use		Matematički kolokvij u Osijeku	Fair use
	Univ. of Warwick	Fair use		Ekin Özman	Fair use
				Univ. of Warwick	Fair use

MFO = Mathematisches Forschungsinstitut Oberwolfach