Explicit isogenies of prime degree over number fields

Barinder Singh Banwait

Harish-Chandra Research Institute

VaNTAGe Seminar
Tuesday, 29th June 2021

VaNTAGe

a virtual math seminar on open conjectures in number theory and arithmetic geometry

Copyright Disclaimer: ***Photo credits and attribution are given in the final section.***

Isogenies

Rational Isogenies

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

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 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.

The Dream

Goal

"Understand rational isogenies."

Fact

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

Reduced Goal

"Understand cyclic rational isogenies."

The Dream made precise

Open Problem

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, so the above Open Problem should be interpreted as:

- Exactly determine $\mathrm{IsogCyclicDeg}(K)$ when it is finite;
- Classify the degrees in $\mathrm{IsogCyclicDeg}(K)$ when it is infinite.

Question

What happens for $K = \mathbb{Q}$?

Mazur’s Method

The Theorems of Mazur and Kenku

Theorem (Mazur, 1978, [Maz78])

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

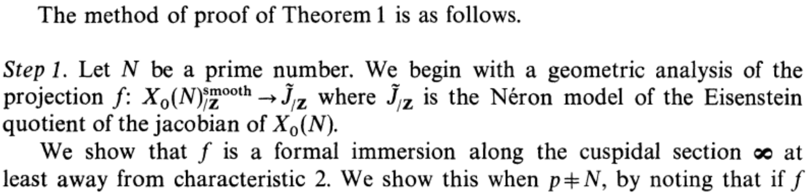
Theorem (Kenku, 1981, [Ken79, Ken80a, Ken80b, Ken81])

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

Barry C. Mazur

Monsur A. Kenku

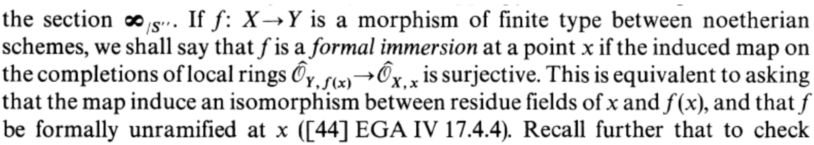
Mazur's Formal Immersion Method



The method of proof of Theorem 1 is as follows.

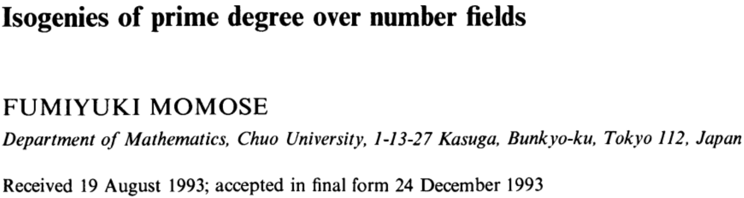
Step 1. Let N be a prime number. We begin with a geometric analysis of the projection $f\colon X_0(N)^{\text{smooth}}_{/\mathbf{Z}} \to \tilde{J}_{/\mathbf{Z}}$ where $\tilde{J}_{/\mathbf{Z}}$ is the Néron model of the Eisenstein quotient of the jacobian of $X_0(N)$.

We show that f is a formal immersion along the cuspidal section $\boldsymbol{\infty}$ at least away from characteristic 2. We show this when $p \neq N$, by noting that if f



the section $\boldsymbol{\infty}_{/S''}$. If $f\colon X \to Y$ is a morphism of finite type between noetherian schemes, we shall say that f is a *formal immersion* at a point x if the induced map on the completions of local rings $\hat{\mathcal{O}}_{Y,f(x)} \to \hat{\mathcal{O}}_{X,x}$ is surjective. This is equivalent to asking that the map induce an isomorphism between residue fields of x and $f(x)$, and that f be formally unramified at x ([44] EGA IV 17.4.4). Recall further that to check

The work of Fumiyuki Momose



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 [Mom95], Momose classified isogenies into three types according to the isogeny character, which encodes the Galois action

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

on the kernel V of a K-rational p-isogeny.

Fumiyuki Momose

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. 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 $\alpha\mathcal{O}_L = \mathrm{Nm}_{K/L}(\mathfrak{q})$.

Type 1 isogenies

Theorem (Momose, Theorem 3 in *loc. cit.*)

Let K be a number field of degree ≤ 12. Then there are only finitely many Type 1 primes for K.

Why the restriction $d := [K : \mathbb{Q}] \leq 12$? The proof requires a formal immersion criterion for the d^{th} symmetric power modular curve:

$$X_0(p)^{(d)} := \overbrace{(X_0(p) \times \cdots \times X_0(p))}^{d\text{-times}} / S_d$$

$$X_0(p)^{(d)} \leftrightarrow \text{effective degree } d \text{ divisors on } X_0(p).$$

Define the map

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

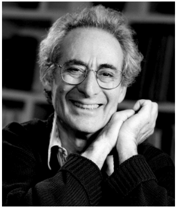
(See [Maz77, Chapter 2 Section 10] for the definition of $\gamma_{\mathfrak{J}}$.)

Theorem (Kamienny, Kamienny-Mazur [KM95], Abramovich [Abr95])

For $d \leq 12$, there are constants A_d and B_d such that, for all primes $p > A_d$ and $q > B_d$, the map $f_p^{(d)}$ is a formal immersion along the section $(\infty, \ldots, \infty)$ in characteristic q.

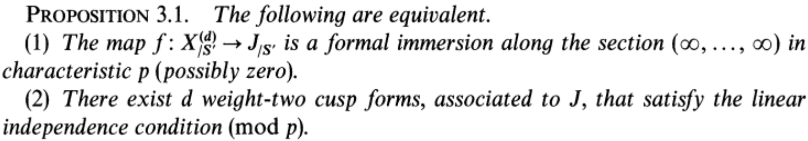
The constants A_d and B_d were not made explicit (except for $d = 2$, more on this later). This theorem was approached via Kamienny's reformulation of the formal immersion criterion in terms of linear independence of Hecke operators in positive characteristic.

Sheldon Kamienny



Barry C. Mazur

Dan Abramovich



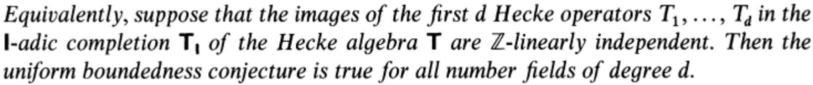
Proposition 3.1. *The following are equivalent.*

(1) *The map $f\colon X^{(d)}_{/S'} \to J_{/S'}$ is a formal immersion along the section* $(\infty, \ldots, \infty)$ *in characteristic p* (*possibly zero*).

(2) *There exist d weight-two cusp forms, associated to J, that satisfy the linear independence condition* (mod p).

from [Kam92b]

Why did they care about such statements?



Equivalently, suppose that the images of the first d Hecke operators $T_1, \ldots, T_d$ in the $\mathbf{l}$*-adic completion* $\mathbf{T}_\mathbf{l}$ *of the Hecke algebra* $\mathbf{T}$ *are* $\mathbb{Z}$*-linearly independent. Then the uniform boundedness conjecture is true for all number fields of degree d.*

from [Kam92b]

We'll revisit this in the 'Merel' section. For now we frame the following:

SLOGAN

Explicit formal immersion criteria defeat Type One primes.

Type 2 isogenies

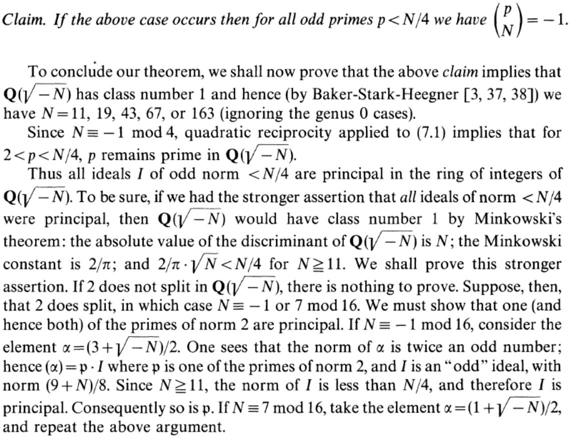
Condition CC (Momose + B.-Derickx)

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

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

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

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



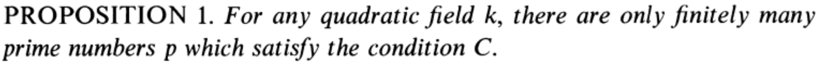
Claim. If the above case occurs then for all odd primes $p < N/4$ we have $\left(\frac{p}{N}\right) = -1$.

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).

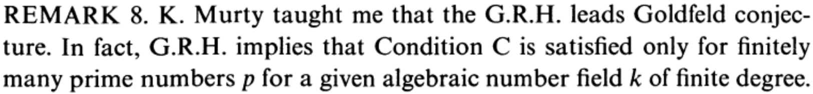
Since $N \equiv -1 \bmod 4$, quadratic reciprocity applied to (7.1) implies that for $2 < p < N/4$, p remains prime in $\mathbf{Q}(\sqrt{-N})$.

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 mod 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.

Determining the Type 2 primes is harder for general K.
However, Momose was able to establish the following two results:



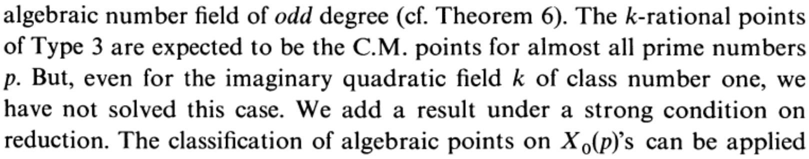
PROPOSITION 1. *For any quadratic field k, there are only finitely many prime numbers p which satisfy the condition C.*



REMARK 8. K. Murty taught me that the G.R.H. leads Goldfeld conjecture. In fact, G.R.H. implies that Condition C is satisfied only for finitely many prime numbers *p* for a given algebraic number field *k* of finite degree.

Vijaya Kumar Murty

Type 3 isogenies



algebraic number field of *odd* degree (cf. Theorem 6). The k-rational points of Type 3 are expected to be the C.M. points for almost all prime numbers p. But, even for the imaginary quadratic field k of class number one, we have not solved this case. We add a result under a strong condition on reduction. The classification of algebraic points on $X_0(p)$'s can be applied

Open Problem (Momose's Conjecture)

Let K be a number field containing the Hilbert class field of an imaginary quadratic field L. Then there is a constant C_K such that, for prime $p > C_K$, if there exists an elliptic curve E over K admitting a K-rational p-isogeny of Type 3, then E has CM by an order $\mathcal{O}$ in L, and p splits or ramifies in $\mathcal{O}$.

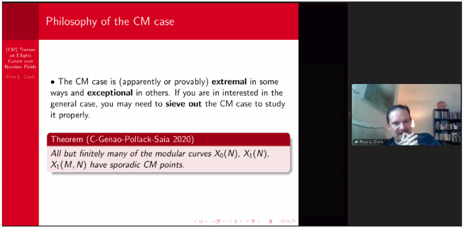
After Lori Watson's talk in this series, I wondered the following:

Question

Does Momose's conjecture follow from recent developments in the realm of isolated or sporadic points on modular curves?

Pete Clark also mentioned "sporadic CM points" which might be relevant here.

One place to start with this is to watch their respective VaNTAGe talks.



Philosophy of the CM case

(CM) Torsion on Elliptic Curves over Number Fields

Pete L. Clark

- The CM case is (apparently or provably) **extremal** in some ways and **exceptional** in others. If you are in interested in the general case, you may need to **sieve out** the CM case to study it properly.

Theorem (C-Genao-Pollack-Saia 2020)

All but finitely many of the modular curves $X_0(N)$, $X_1(N)$, $X_1(M,N)$ have sporadic CM points.

Pete L. Clark
VaNTAGe talk:

`https://youtu.be/4cX8amfVr8M`

Lori D. Watson
VaNTAGe talk:

`https://youtu.be/S4ZX3CUIzLE`

In summary ...

Theorem (Momose)

Assume GRH. Let K be a number field of degree ≤ 12 which does not contain the Hilbert class field of an imaginary quadratic field. Then $\mathrm{IsogPrimeDeg}(K)$ *is finite.*

Theorem (Momose)

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

These results of Momose were not effective.

Question

Can one exactly determine $\mathrm{IsogPrimeDeg}(K)$ *for a single number field* $K \neq \mathbb{Q}$*?*

The work of Loïc Merel

Strong Uniform Boundedness for torsion on elliptic curves

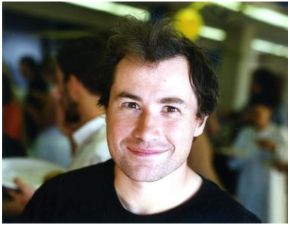
Conjecture

Let $d \geq 1$ be an integer. Then there is a constant B_d such that, if E is an elliptic curve over any number field K of degree $\leq d$, then $|E(K)_{tors}| \leq B_d$.

Strong Uniform Boundedness for torsion on elliptic curves

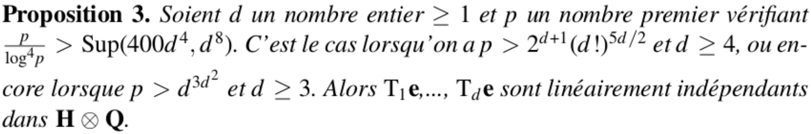
Theorem (Merel, 1996, [Mer96])

Let $d \geq 1$ be an integer. Then there is a constant B_d such that, if E is an elliptic curve over any number field K of degree $\leq d$, then $|E(K)_{tors}| \leq B_d$.



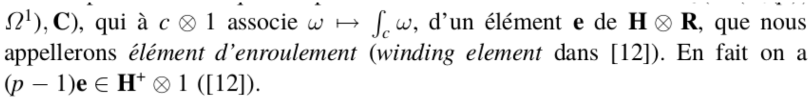
Loïc Merel

Merel proved the linear independence of Hecke operators for general d:



Proposition 3. *Soient d un nombre entier ≥ 1 et p un nombre premier vérifiant $\frac{p}{\log^4 p} > \mathrm{Sup}(400d^4, d^8)$. C'est le cas lorsqu'on a $p > 2^{d+1}(d!)^{5d/2}$ et $d \geq 4$, ou encore lorsque $p > d^{3d^2}$ et $d \geq 3$. Alors $\mathrm{T}_1\mathbf{e}, \ldots, \mathrm{T}_d\mathbf{e}$ sont linéairement indépendants dans $\mathbf{H} \otimes \mathbf{Q}$.*

This was achieved by working with the Winding quotient rather than the Eisenstein quotient.



Ω^1), **C**), qui à $c \otimes 1$ associe $\omega \mapsto \int_c \omega$, d'un élément **e** de $\mathbf{H} \otimes \mathbf{R}$, que nous appellerons *élément d'enroulement* (*winding element* dans [12]). En fait on a $(p-1)\mathbf{e} \in \mathbf{H}^+ \otimes 1$ ([12]).

The winding quotient is the largest rank 0 quotient of $J_0(N)$, and it allows one to get **explicit formal immersion criteria** (i.e. the A_d and B_d from earlier can be written down).

In summary ...

Theorem (Momose)

Assume GRH. Let K be a number field of degree ≤ 12 which does not contain the Hilbert class field of an imaginary quadratic field. Then $\mathrm{IsogPrimeDeg}(K)$ *is finite.*

Theorem (Momose)

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

These results of Momose were not effective.

Question

Can one exactly determine $\mathrm{IsogPrimeDeg}(K)$ *for a single number field $K \neq \mathbb{Q}$?*

In summary ...

Theorem (Momose + Merel)

Assume GRH. Let K be a number field ~~of degree ≤ 12~~ which does not contain the Hilbert class field of an imaginary quadratic field. Then $\mathrm{IsogPrimeDeg}(K)$ *is finite.*

Theorem (Momose)

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

These results of Momose were not effective.

Question

Can one exactly determine $\mathrm{IsogPrimeDeg}(K)$ *for a single number field $K \neq \mathbb{Q}$?*

Explicit isogenies of prime degree over quadratic fields

arxiv.org/abs/2101.02673 - submitted

Question

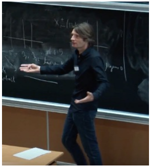
Can one exactly determine IsogPrimeDeg(K) *for a single number field* $K \neq \mathbb{Q}$*?*

Makes sense to start at quadratic fields K which are not imaginary quadratic of class number one (called isogeny-finite in the sequel). I tried to approach this via a two-step process:

1. Find an upper bound for IsogPrimeDeg(K);
2. For each prime up to this upper bound, decide whether or not it is in IsogPrimeDeg(K).

Note that this is the same approach used by Yuri Bilu, Pierre Parent, and Marusia Rebolledo to show that the split Cartan primes over the rationals are $\{2, 3, 5, 7, 13\}$ [BPR13].

Yuri Bilu



Pierre Parent

Marusia Rebolledo

Upper bound for IsogPrimeDeg(K)

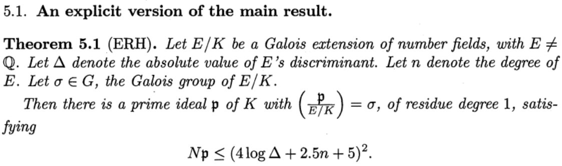
There are 3 components of IsogPrimeDeg(K):

	C_0	TypeOnePrimes	TypeTwoPrimes	
Bound	$C(K, 2(\Delta_K)^{Ah_K})$	$(1 + 3^{6d_K h_K})^2$	$\prod_{\ell \in S_K} \ell \leq e^{c_2^{d_K}(R_K d_K^{r_K} + (h_K \log \Delta_K)^2)}$	
Found by	Agnès David	Joseph Oesterlé	Eric Larson & Dmitry Vaintrob	
Reference	[Dav12]	[DKSS17, Section 6]	[LV14]	

This wasn't quite explicit because of the unknown constants A and c_2 which arise from applying Effective Chebotarev Density.

However, we replaced these steps with the absolute best possible Effective Chebotarev Density bound of Bach and Sorenson [BS96] (which is free of unknown constants):

Eric Bach



5.1. **An explicit version of the main result.**

Theorem 5.1 (ERH). *Let E/K be a Galois extension of number fields, with $E \neq \mathbb{Q}$. Let Δ denote the absolute value of E's discriminant. Let n denote the degree of E. Let $\sigma \in G$, the Galois group of E/K.*

Then there is a prime ideal $\mathfrak{p}$ of K with $\left(\frac{\mathfrak{p}}{E/K}\right) = \sigma$, of residue degree 1, satisfying

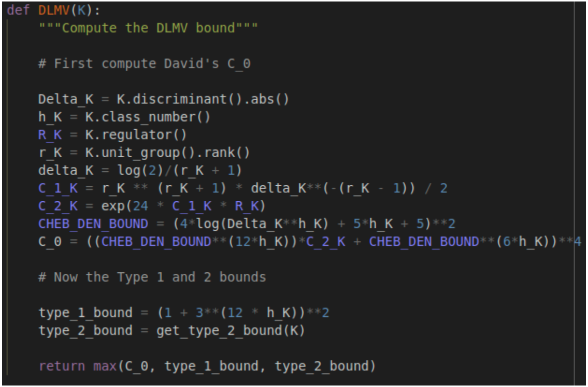
$$N\mathfrak{p} \leq (4 \log \Delta + 2.5n + 5)^2.$$

Jonathan Sorenson

The DLMV bound

Proposition (B.)

Assume GRH. Then there is an algorithm which, given a quadratic field K which is not imaginary quadratic of class number 1, computes an upper bound on $\mathrm{IsogPrimeDeg}(K)$.



```
def DLMV(K):
    """Compute the DLMV bound"""

    # First compute David's C_0

    Delta_K = K.discriminant().abs()
    h_K = K.class_number()
    R_K = K.regulator()
    r_K = K.unit_group().rank()
    delta_K = log(2)/(r_K + 1)
    C_1_K = r_K ** (r_K + 1) * delta_K**(-(r_K - 1)) / 2
    C_2_K = exp(24 * C_1_K * R_K)
    CHEB_DEN_BOUND = (4*log(Delta_K**h_K) + 5*h_K + 5)**2
    C_0 = ((CHEB_DEN_BOUND**(12*h_K))*C_2_K + CHEB_DEN_BOUND**(6*h_K))**4

    # Now the Type 1 and 2 bounds

    type_1_bound = (1 + 3**(12 * h_K))**2
    type_2_bound = get_type_2_bound(K)

    return max(C_0, type_1_bound, type_2_bound)
```

Δ_K	K	$\mathrm{DLMV}(K)$
-40	$\mathbb{Q}(\sqrt{-10})$	3.20×10^{316}
-24	$\mathbb{Q}(\sqrt{-6})$	2.99×10^{308}
-20	$\mathbb{Q}(\sqrt{-5})$	2.58×10^{305}
8	$\mathbb{Q}(\sqrt{2})$	4.06×10^{139}
12	$\mathbb{Q}(\sqrt{3})$	1.68×10^{152}
5	$\mathbb{Q}(\sqrt{5})$	5.65×10^{126}
24	$\mathbb{Q}(\sqrt{6})$	9.76×10^{177}
28	$\mathbb{Q}(\sqrt{7})$	1.08×10^{189}
40	$\mathbb{Q}(\sqrt{10})$	2.59×10^{354}

Clearly the bounds had to be improved ... so I returned to Momose's paper ... *after 10 years!*

The backstory

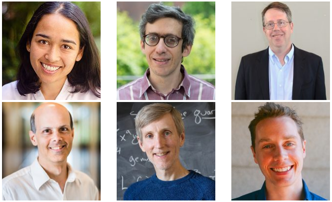
John Cremona suggests the problem to me in about June 2010.

Jim Stankewicz tells me about Momose's paper in about November 2010.

In June 2020 I attend the Simons AGNTC workshop organised by Jennifer Balakrishnan, Noam Elkies, Brendan Hassett, Bjorn Poonen, Drew Sutherland, and John Voight.

John Cremona

Jim Stankewicz and I take selfie with Bryan Birch



The organisers of Simons AGNTC 2020

On the first day of that workshop I have a zoom call with Isabel Vogt who clearly explains to me an idea of Luis Dieulefait who has a method to compute *non-surjective primes* of a generic genus 2 curve over $\mathbb{Q}$ [Die02].

Very roughly, the idea is to choose a finite set of auxiliary primes q, compute a handful of integers $A_i(q)$ whose supports in union is a superset for the non-surjective primes, then take GCDs over q of the LCMs of $A_i(q)$.

Isabel Vogt

Luis V. Dieulefait

Back to the problem ...

When I returned to Momose's paper in November 2020, I had the following question in mind:

Question

Instead of finding upper bounds for IsogPrimeDeg(K)*, can you instead find a tight superset for it by computing a handful of integers associated to auxiliary primes* $\mathfrak{q}$ *of* K*?*

This led to the integers

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

See the paper for the definitions, or attend my up upcoming talk at Universität Bayreuth:
`http://www.mathe2.uni-bayreuth.de/oberseminar/index.html`

Coding it all up led to

Theorem (B.)

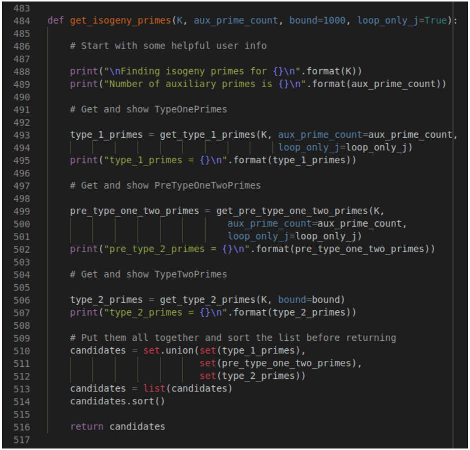
Let K be a quadratic field which is not imaginary quadratic of class number 1. Then there is an algorithm which computes a superset of $\mathrm{IsogPrimeDeg}(K)$ *as the union of three sets:*

$$\begin{aligned}\mathrm{IsogPrimeDeg}(K) \subseteq \mathrm{PreTypeOneTwoPrimes}(K) &\cup \mathrm{TypeOnePrimes}(K)\\ &\cup \mathrm{TypeTwoPrimes}(K).\end{aligned}$$

Quadratic Isogeny Primes

Sage and PARI/GP implementation of the command-line tool is 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

```

TypeOnePrimes

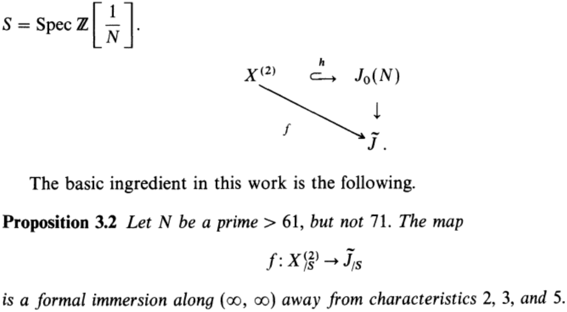
Recalling that

SLOGAN

Explicit formal immersion criteria defeat Type One primes.

we use Kamienny's explicit formal immersion criteria for quadratic fields:

Sheldon Kamienny



$$S = \operatorname{Spec} \mathbb{Z}\left[\frac{1}{N}\right].$$

$$\begin{tikzcd} X^{(2)} \arrow[r, hook, "h"] \arrow[dr, "f"'] & J_0(N) \arrow[d] \\ & \tilde{J}\,. \end{tikzcd}$$

The basic ingredient in this work is the following.

Proposition 3.2 *Let N be a prime > 61, but not 71. The map*

$$f\colon X^{(2)}_{/S} \to \tilde{J}_{/S}$$

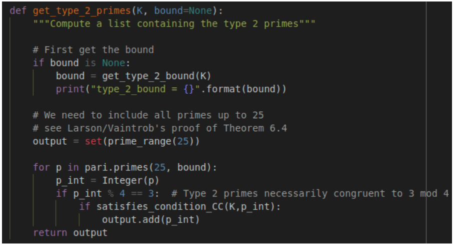
is a formal immersion along (∞, ∞) *away from characteristics* 2, 3, *and* 5.

From [Kam92a].

$$\begin{aligned}\mathrm{TypeOnePrimes}(K) = \mathrm{PrimesUpTo}(71) &\cup \{p : p \mid \Delta_K\} \\ &\cup \{p : (p-1) \mid 12h_K\} \cup \left(\bigcap_{\mathfrak{q} \in \mathrm{Aux}} \{p : p \mid D(\mathfrak{q})\} \right).\end{aligned}$$

TypeTwoPrimes

This part of the algorithm doesn't use auxiliary primes, but instead checks primes up to the bound on TypeTwoPrimes whether they satisfy condition CC:

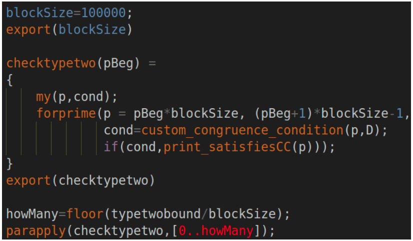


```python
def get_type_2_primes(K, bound=None):
    """Compute a list containing the type 2 primes"""

    # 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]);
```

From Superset to Set

Let's run the algorithm on $\mathbb{Q}(\sqrt{5})$; we get a superset of

$$\mathrm{PrimesUpTo}(79) \cup \{163\} .$$

How to determine which of these are actually in $\mathrm{IsogPrimeDeg}(\mathbb{Q}(\sqrt{5}))$?

There are three ingredients.

Ingredient 1: Quadratic points on low-genus modular curves

Peter J. Bruin

Hyperelliptic modular curves $X_0(N)$ and isogenies of elliptic curves over quadratic fields, 2015 [BN15]

Filip Najman

Ekin Özman

Quadratic points on modular curves, 2019 [ÖS19], see Ekin's VaNTAGe talk here: `https://youtu.be/fj--cM2o-sA`

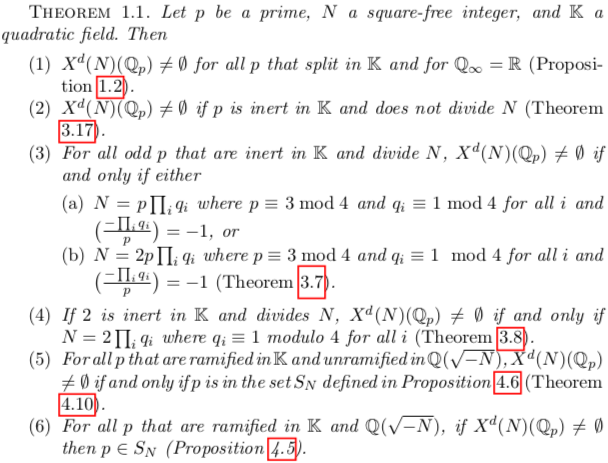
Samir Siksek

Josha Box

Quadratic points on modular curves with infinite Mordell-Weil group, 2021 [Box21]

Ingredient 2: Local solubility of twisted modular curves

Ekin Özman



THEOREM 1.1. *Let p be a prime, N a square-free integer, and $\mathbb{K}$ a quadratic field. Then*

(1) *$X^d(N)(\mathbb{Q}_p) \neq \emptyset$ for all p that split in $\mathbb{K}$ and for $\mathbb{Q}_\infty = \mathbb{R}$* (Proposition 1.2).

(2) *$X^d(N)(\mathbb{Q}_p) \neq \emptyset$ if p is inert in $\mathbb{K}$ and does not divide N* (Theorem 3.17).

(3) *For all odd p that are inert in $\mathbb{K}$ and divide N, $X^d(N)(\mathbb{Q}_p) \neq \emptyset$ if and only if either*

(a) *$N = p\prod_i q_i$ where $p \equiv 3 \bmod 4$ and $q_i \equiv 1 \bmod 4$ for all i and $\left(\frac{-\prod_i q_i}{p}\right) = -1$, or*

(b) *$N = 2p\prod_i q_i$ where $p \equiv 3 \bmod 4$ and $q_i \equiv 1 \mod 4$ for all i and $\left(\frac{-\prod_i q_i}{p}\right) = -1$* (Theorem 3.7).

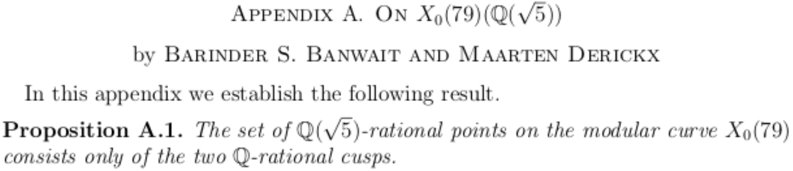
(4) *If 2 is inert in $\mathbb{K}$ and divides N, $X^d(N)(\mathbb{Q}_p) \neq \emptyset$ if and only if $N = 2\prod_i q_i$ where $q_i \equiv 1$ modulo 4 for all i* (Theorem 3.8).

(5) *For all p that are ramified in $\mathbb{K}$ and unramified in $\mathbb{Q}(\sqrt{-N})$, $X^d(N)(\mathbb{Q}_p) \neq \emptyset$ if and only if p is in the set S_N defined in Proposition 4.6* (Theorem 4.10).

(6) *For all p that are ramified in $\mathbb{K}$ and $\mathbb{Q}(\sqrt{-N})$, if $X^d(N)(\mathbb{Q}_p) \neq \emptyset$ then $p \in S_N$ (Proposition 4.5).*

From [Özm12]

Ingredient 3: Dealing with 79



Appendix A. On $X_0(79)(\mathbb{Q}(\sqrt{5}))$

by Barinder S. Banwait and Maarten Derickx

In this appendix we establish the following result.

Proposition A.1. *The set of $\mathbb{Q}(\sqrt{5})$-rational points on the modular curve $X_0(79)$ consists only of the two $\mathbb{Q}$-rational cusps.*

Maarten Derickx

This requires that

$$J_0(79)_-(\mathbb{Q}(\sqrt{5})) = J_0(79)_-(\mathbb{Q}).$$

We in fact show that $J_0(79)_-(\mathbb{Q})_{tors}$ does not grow in any quadratic extension.

Open Problem (Quadratic Generalised Ogg's conjecture?)

In general how does the torsion of $J_0(N)$ grow from $\mathbb{Q}$ to (specific) quadratic fields? What about the minus part?

See [Yoo21] for recent progress on the Generalised Ogg conjecture over $\mathbb{Q}$.

Hwajong Yoo

To summarise...

Theorem (B.)

Assuming GRH, we have the following.

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

Open Problem

Can you extend the results on quadratic points on low-genus modular curves to higher genera?

Work in progress with Maarten Derickx

Theorem (B.-Derickx)

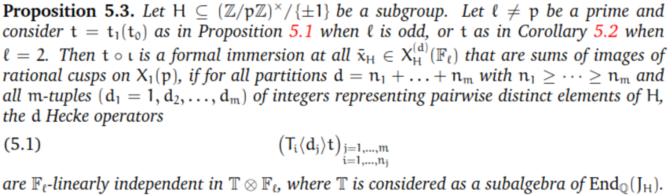
Let K be a number field which does not contain the Hilbert class field of an imaginary quadratic field. Then there is an algorithm which computes a superset of $\mathrm{IsogPrimeDeg}(K)$ *as the union of three sets:*

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

Zoom call with Maarten Derickx

TypeOnePrimes

The implementation of TypeOnePrimes uses the state-of-the-art explicit and tight formal immersion criteria due to Derickx, Kamienny, Stein, and Stoll [DKSS17]:



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

From Superset to Set

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

$$\mathrm{PrimesUpTo}(43) \cup \{61, 67, 73, 163\}.$$

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 [BGG21].

Josha Box

Stevan Gajović

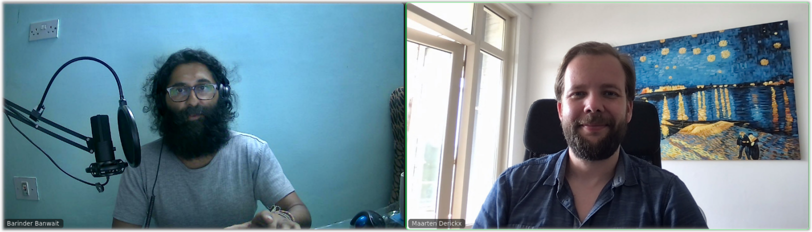
Pip Goodman

The first cubic case of IsogPrimeDeg

Theorem (B.-Derickx)

Assuming GRH,

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



Open Problem

Can you extend the results on cubic points on low-genus modular curves to higher genera?

Open Problem

Can you start compiling catalogues of higher degree points on low-genus modular curves?

Uniform TypeTwoPrimes

Theorem (B.-Derickx)

Assume GRH, and let d be an odd integer. Then there is a bound C_d such that if E is an elliptic curve over a number field K of degree d which admits a K-rational p-isogeny, then $p \leq C_d$. Moreover, we have $C_3 = 253{,}507$.

There *is* a cubic field which satisfies Condition CC with $p = 253{,}507$, but this is only a necessary condition for Type 2 isogenies, so the following is natural:

Open Problem

Does there exist an elliptic curve over a cubic field admitting a rational 253,507-isogeny?

Strong Uniform Boundedness for Isogenies?

Open Problem

Fix an integer d. As one varies over all elliptic curves over all number fields of degree d which do not contain the Hilbert class field of an imaginary quadratic field, are there only finitely many isogeny primes that arise?

Code optimisations

Bill Allombert

"Tu devrais essayer GP2C, GP2C est plus rapide que GP pour les boucles longues."

reproduced with permission

Open Problem

*Can you make the implementation **wicked fast**?*

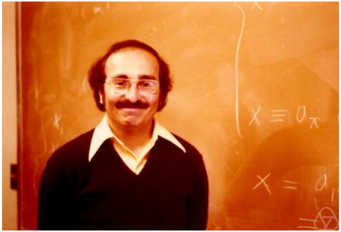
Further Problems to consider

Statistical Distribution of IsogPrimeDeg(K)

Both Ralph Greenberg and Jaap Top asked this *Arithmetic Statistics* question:

Open Problem

Fix an integer d. What is the distribution of IsogPrimeDeg(K) *as one varies over all number fields K of degree d?*



Ralph Greenberg

Jaap Top

Definition

Let K be a number field, and let $p \in \mathrm{IsogPrimeDeg}(K)$. We say that p is **new** if $p \notin \mathrm{IsogPrimeDeg}(L)$ for any proper subfield $L \subset K$.

Question

As one varies over all isogeny-finite quadratic fields $\mathbb{Q}(\sqrt{D})$ for $|D| \leq 50$, how many new isogeny primes arise for each D, which new isogeny primes arise, and how often do they arise?

There are 54 quadratic fields to consider.
We were able to decide on 38 of these.

Theorem (B.-Derickx)

Assuming GRH,

$\mathbf{IsogPrimeDeg}(\mathbb{Q}(\sqrt{-46})) = \mathbf{IsogPrimeDeg}(\mathbb{Q})$

$\mathbf{IsogPrimeDeg}(\mathbb{Q}(\sqrt{-42})) = \mathbf{IsogPrimeDeg}(\mathbb{Q})$

$\mathbf{IsogPrimeDeg}(\mathbb{Q}(\sqrt{-39})) = \mathbf{IsogPrimeDeg}(\mathbb{Q})$

$\mathbf{IsogPrimeDeg}(\mathbb{Q}(\sqrt{-38})) = \mathbf{IsogPrimeDeg}(\mathbb{Q})$

$\mathbf{IsogPrimeDeg}(\mathbb{Q}(\sqrt{-34})) = \mathbf{IsogPrimeDeg}(\mathbb{Q})$

$\mathbf{IsogPrimeDeg}(\mathbb{Q}(\sqrt{-30})) = \mathbf{IsogPrimeDeg}(\mathbb{Q})$

$\mathbf{IsogPrimeDeg}(\mathbb{Q}(\sqrt{-29})) = \mathbf{IsogPrimeDeg}(\mathbb{Q})$

$\mathbf{IsogPrimeDeg}(\mathbb{Q}(\sqrt{-23})) = \mathbf{IsogPrimeDeg}(\mathbb{Q}) \cup \{\mathbf{29}, \mathbf{31}\}$

$\mathbf{IsogPrimeDeg}(\mathbb{Q}(\sqrt{-21})) = \mathbf{IsogPrimeDeg}(\mathbb{Q})$

$\mathbf{IsogPrimeDeg}(\mathbb{Q}(\sqrt{-17})) = \mathbf{IsogPrimeDeg}(\mathbb{Q})$

$\mathbf{IsogPrimeDeg}(\mathbb{Q}(\sqrt{-15})) = \mathbf{IsogPrimeDeg}(\mathbb{Q}) \cup \{\mathbf{23}\}$

$\mathbf{IsogPrimeDeg}(\mathbb{Q}(\sqrt{-14})) = \mathbf{IsogPrimeDeg}(\mathbb{Q})$

$\mathbf{IsogPrimeDeg}(\mathbb{Q}(\sqrt{-13})) = \mathbf{IsogPrimeDeg}(\mathbb{Q})$

$\mathbf{IsogPrimeDeg}(\mathbb{Q}(\sqrt{-5})) = \mathbf{IsogPrimeDeg}(\mathbb{Q}) \cup \{\mathbf{23}\}$

$\mathbf{IsogPrimeDeg}(\mathbb{Q}(\sqrt{2})) = \mathbf{IsogPrimeDeg}(\mathbb{Q})$

$\mathbf{IsogPrimeDeg}(\mathbb{Q}(\sqrt{3})) = \mathbf{IsogPrimeDeg}(\mathbb{Q})$

$\mathbf{IsogPrimeDeg}(\mathbb{Q}(\sqrt{6})) = \mathbf{IsogPrimeDeg}(\mathbb{Q})$

$\mathbf{IsogPrimeDeg}(\mathbb{Q}(\sqrt{7})) = \mathbf{IsogPrimeDeg}(\mathbb{Q})$

$\mathbf{IsogPrimeDeg}(\mathbb{Q}(\sqrt{10})) = \mathbf{IsogPrimeDeg}(\mathbb{Q})$

$\mathbf{IsogPrimeDeg}(\mathbb{Q}(\sqrt{11})) = \mathbf{IsogPrimeDeg}(\mathbb{Q})$

$\mathbf{IsogPrimeDeg}(\mathbb{Q}(\sqrt{13})) = \mathbf{IsogPrimeDeg}(\mathbb{Q}) \cup \{\mathbf{31}\}$

$\mathbf{IsogPrimeDeg}(\mathbb{Q}(\sqrt{14})) = \mathbf{IsogPrimeDeg}(\mathbb{Q})$

$\mathbf{IsogPrimeDeg}(\mathbb{Q}(\sqrt{19})) = \mathbf{IsogPrimeDeg}(\mathbb{Q})$

$\mathbf{IsogPrimeDeg}(\mathbb{Q}(\sqrt{21})) = \mathbf{IsogPrimeDeg}(\mathbb{Q})$

$\mathbf{IsogPrimeDeg}(\mathbb{Q}(\sqrt{23})) = \mathbf{IsogPrimeDeg}(\mathbb{Q})$

$\mathbf{IsogPrimeDeg}(\mathbb{Q}(\sqrt{26})) = \mathbf{IsogPrimeDeg}(\mathbb{Q})$

$\mathbf{IsogPrimeDeg}(\mathbb{Q}(\sqrt{30})) = \mathbf{IsogPrimeDeg}(\mathbb{Q})$

$\mathbf{IsogPrimeDeg}(\mathbb{Q}(\sqrt{31})) = \mathbf{IsogPrimeDeg}(\mathbb{Q})$

$\mathbf{IsogPrimeDeg}(\mathbb{Q}(\sqrt{33})) = \mathbf{IsogPrimeDeg}(\mathbb{Q})$

$\mathbf{IsogPrimeDeg}(\mathbb{Q}(\sqrt{34})) = \mathbf{IsogPrimeDeg}(\mathbb{Q})$

$\mathbf{IsogPrimeDeg}(\mathbb{Q}(\sqrt{35})) = \mathbf{IsogPrimeDeg}(\mathbb{Q})$

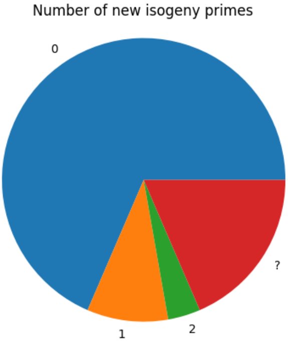
$\mathbf{IsogPrimeDeg}(\mathbb{Q}(\sqrt{38})) = \mathbf{IsogPrimeDeg}(\mathbb{Q})$

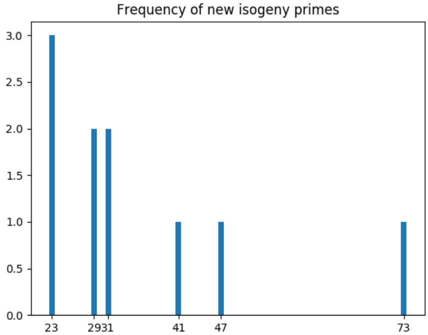
$\mathbf{IsogPrimeDeg}(\mathbb{Q}(\sqrt{39})) = \mathbf{IsogPrimeDeg}(\mathbb{Q})$

$\mathbf{IsogPrimeDeg}(\mathbb{Q}(\sqrt{42})) = \mathbf{IsogPrimeDeg}(\mathbb{Q})$

$\mathbf{IsogPrimeDeg}(\mathbb{Q}(\sqrt{43})) = \mathbf{IsogPrimeDeg}(\mathbb{Q})$

$\mathbf{IsogPrimeDeg}(\mathbb{Q}(\sqrt{46})) = \mathbf{IsogPrimeDeg}(\mathbb{Q})$





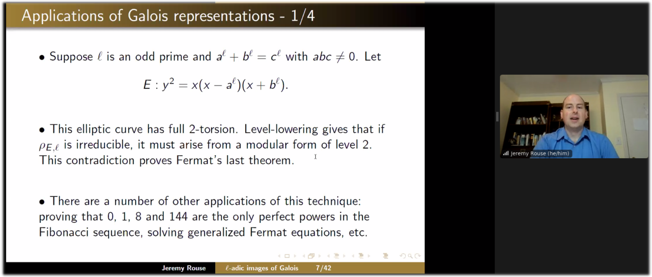
OK, to be totally honest: In these diagrams I have assumed that the hyperelliptic curves $X^{17}(23)$, $X^{37}(23)$, $X^{29}(31)$, $X^{29}(37)$, $X^{-31}(41)$, $X^{-22}(59)$, $X^{47}(59)$ do not have any $\mathbb{Q}$-rational points, because I searched up to a really big height bound but failed to find any points. This could possibly be proved with Quadratic Chabauty; this only affects a small number of the 54 cases, so even if not true, the general picture would remain unaffected.

Put results in `https://lmfdb.org`?

Question

Do people want to see the results in the LMFDB*? Even if they're "only supersets"?*

See Jeremy Rouse's VaNTAGe talk for applications of knowing what the isogeny primes are.

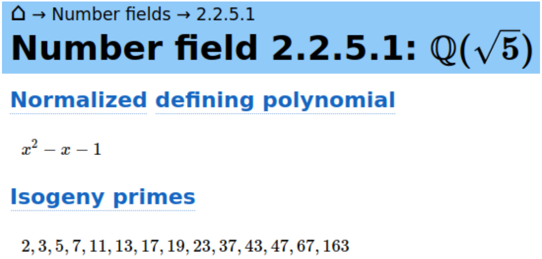


Applications of Galois representations - 1/4

- Suppose ℓ is an odd prime and $a^\ell + b^\ell = c^\ell$ with $abc \neq 0$. Let
$$E : y^2 = x(x - a^\ell)(x + b^\ell).$$
- This elliptic curve has full 2-torsion. Level-lowering gives that if $\rho_{E,\ell}$ is irreducible, it must arise from a modular form of level 2. This contradiction proves Fermat's last theorem.
- There are a number of other applications of this technique: proving that 0, 1, 8 and 144 are the only perfect powers in the Fibonacci sequence, solving generalized Fermat equations, etc.

Jeremy Rouse ℓ-adic images of Galois 7/42

Jeremy Rouse's VaNTAGe talk: `https://youtu.be/L_Il_sJymEs`



⌂ → Number fields → 2.2.5.1

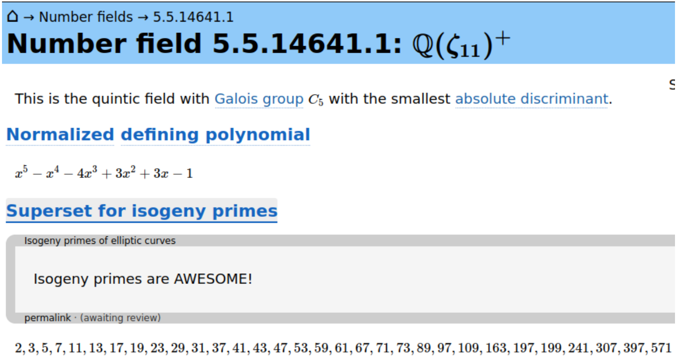
Number field 2.2.5.1: $\mathbb{Q}(\sqrt{5})$

Normalized defining polynomial

$x^2 - x - 1$

Isogeny primes

$2, 3, 5, 7, 11, 13, 17, 19, 23, 37, 43, 47, 67, 163$



⌂ → Number fields → 5.5.14641.1

Number field 5.5.14641.1: $\mathbb{Q}(\zeta_{11})^+$

This is the quintic field with Galois group C_5 with the smallest absolute discriminant.

Normalized defining polynomial

$x^5 - x^4 - 4x^3 + 3x^2 + 3x - 1$

Superset for isogeny primes

Isogeny primes of elliptic curves

Isogeny primes are AWESOME!

permalink · (awaiting review)

$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 89, 97, 109, 163, 197, 199, 241, 307, 397, 571$

Quadratic Bilu-Parent-Rebolledo?

Momose wrote a paper about the split Cartan modular curves $X_s(p)$ [Mom84] and one about its generalisation $X_0^+(p^r)$ [Mom87].

Open Problem

Fix a quadratic field K. Can one exactly determine the primes p for which the split Cartan modular curve $X_s(p)$ admits non-cuspidal, non-CM rational points?

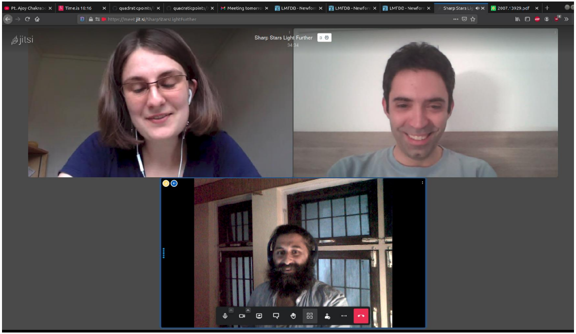
There's been enough progress on quadratic points on modular curves in recent years to at least start thinking about this seriously.

Quadratic Kenku

Open Problem

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

I am currently working on this with Oana Adascalitei and Filip Najman:



Mazur's theorems for abelian surfaces?

Open Problem

Is there a uniform bound on isogeny primes for abelian surfaces over $\mathbb{Q}$?

Open Problem

Is there a uniform bound on torsion primes for abelian surfaces over $\mathbb{Q}$?

One may initially want to restrict the class to principally polarised abelian surfaces, and to isogenies which are compatible with the polarisation. But this is hard because fewer explicit results are known about moduli spaces of principally polarised abelian surfaces.

Thank You!

Thanks for listening!

MFO = Mathematisches Forschungsinstitut Oberwolfach

Image	Copyright Holder	License
	George M. Bergman, via MFO	CC BY-SA 2.0
	George M. Bergman, via MFO	CC BY-SA 2.0
	Harvard University	Fair use
	Univ. of Washington	Fair use
	Eric Bach	Fair use
	Peter J. Bruin	Fair use
	ResearchGate	Fair use
	Univ. of Warwick	Fair use
	Wake Forest Univ.	Fair use
	Pip Goodman	Fair use

Image	Copyright Holder	License
	Math. Dept., Chuo University, Tokyo, Japan	Fair use
	Univ. Southern California	Fair use
	Getty images/Jewel Samad	Fair use (embed)
	Dmitry Vaintrob	Fair use
	Butler College	Fair use
	Matematički kolokvij u Osijeku	Fair use
	Ekin Özman	Fair use
	Univ. of Warwick	Fair use
	Bill Allombert	Permission obtained
	Dan Abramovich	Fair use
	Kumar Murty	Fair use
	MFO	CC BY-SA 2.0

CIRM = Centre International de Rencontres Mathématiques MFO = Mathematisches Forschungsinstitut Oberwolfach

Image	Copyright Holder	License
	George M. Bergman, via MFO	CC BY-SA 2.0
	CIRM	CC BY-NC-ND 2.0
	Institut de Mathématiques de Marseilles	Fair use
	Univ. of Warwick	Fair use
	Jennifer S. Balakrishnan	Fair use
	Noam Elkies	Fair use
	Brendan Hassett	Fair use
	Joe Rabinoff	Fair use
	Luis V. Dieulefait	Fair use
	Maarten Derickx	Permission obtained
	William Stein	Fair use
	LinkedIn	Fair use

Image	Copyright Holder	License
	Yuri Bilu	Fair use
	Marusia Rebolledo	Permission obtained
	George M. Bergman, via MFO	CC BY-SA 2.0
	Bjorn Poonen	Fair use
	Andrew V. Sutherland	Fair use
	John Voight	Fair use
	Univ. Southern California	Fair use
	Hwajong Yoo	Fair use
	Michael Stoll	Fair use
	ResearchGate	Fair use
	Rijksuniversiteit Groningen	Fair use

[Abr95] Dan Abramovich.
Formal finiteness and the torsion conjecture on elliptic curves.
Astérisque, (228):5–18, 1995.

[Ban21] Barinder S. Banwait.
Explicit isogenies of prime degree over quadratic fields.
submitted. Preprint available online at https://arxiv.org/abs/2101.02673, 2021.

[BGG21] Josha Box, Stevan Gajović, and Pip Goodman.
Cubic and quartic points on modular curves using generalised symmetric Chabauty.
Preprint available online at https://arxiv.org/abs/2102.08236, 2021.

[BN15] Peter Bruin and Filip Najman.
Hyperelliptic modular curves $X_0(n)$ and isogenies of elliptic curves over quadratic fields.
LMS Journal of Computation and Mathematics, 18(1):578–602, 2015.

[Box21] Josha Box.
Quadratic points on modular curves with infinite Mordell–Weil group.
Mathematics of Computation, 90:321–343, 2021.

[BPR13] Yuri Bilu, Pierre Parent, and Marusia Rebolledo.
Rational points on $X_0^+(p^r)$.
Ann. Inst. Fourier (Grenoble), 63(3):957–984, 2013.

[BS96] Eric Bach and Jonathan Sorenson.
Explicit bounds for primes in residue classes.
Mathematics of Computation, 65(216):1717–1735, 1996.

[Dav12] Agnès David.
Caractère d'isogénie et critères d'irréductibilité.
Preprint available online at https://arxiv.org/abs/1103.3892, 2012.

[Die02] Luis V. Dieulefait.
Explicit determination of the images of the Galois representations attached to abelian surfaces with $\mathrm{End}(A) = \mathbb{Z}$.
Experimental Mathematics, 11(4):503–512, 2002.

[DKSS17] Maarten Derickx, Sheldon Kamienny, William Stein, and Michael Stoll.
Torsion points on elliptic curves over number fields of small degree.
Preprint available online at https://arxiv.org/abs/1707.00364, 2017.

[Kam92a] Sheldon Kamienny.
Torsion points on elliptic curves and q-coefficients of modular forms.
Inventiones mathematicae, 109(1):221–229, 1992.

[Kam92b] Sheldon Kamienny.
Torsion points on elliptic curves over fields of higher degree.
International Mathematics Research Notices, 1992(6):129–133, 1992.

[Ken79] M.A. Kenku.
The modular curve $X_0(39)$ and rational isogeny.
In *Mathematical Proceedings of the Cambridge Philosophical Society*, volume 85, pages 21–23. Cambridge University Press, 1979.

[Ken80a] M.A. Kenku.
The modular curve $X_0(169)$ and rational isogeny.
Journal of the London Mathematical Society, 2(2):239–244, 1980.

[Ken80b] M.A. Kenku.
The modular curves $X_0(65)$ and $X_0(91)$ and rational isogeny.
In *Mathematical Proceedings of the Cambridge Philosophical Society*, volume 87, pages 15–20. Cambridge University Press, 1980.

[Ken81] M.A. Kenku.
On the modular curves $X_0(125)$, $X_1(25)$, and $X_1(49)$.
Journal of the London Mathematical Society, 2(3):415–427, 1981.

[KM95] Sheldon Kamienny and Barry Mazur.
Rational torsion of prime order in elliptic curves over number fields.
Astérisque, 228:81–100, 1995.
With an appendix by Andrew Granville.

[LV14] Eric Larson and Dmitry Vaintrob.
Determinants of subquotients of Galois representations associated with abelian varieties.
Journal of the Institute of Mathematics of Jussieu, 13(3):517–559, 2014.

[Maz77] Barry Mazur.
Modular curves and the Eisenstein ideal.
Publications Mathématiques de l'Institut des Hautes Études Scientifiques, 47(1):33–186, 1977.
With an appendix by Barry Mazur and Michael Rapoport.

[Maz78] Barry Mazur.
Rational isogenies of prime degree.
Inventiones mathematicae, 44(2):129–162, 1978.
With an appendix by Dorian Goldfeld.

[Mer96] Loïc Merel.
Bornes pour la torsion des courbes elliptiques sur les corps de nombres.
Inventiones mathematicae, 124(1-3):437–449, 1996.

[Mom84] Fumiyuki Momose.
Rational points on the modular curves $X_{split}(p)$.
Compositio Mathematica, 52(1):115–137, 1984.

[Mom87] Fumiyuki Momose.
Rational points on the modular curves $X_0^+(N)$.
Journal of the Mathematical Society of Japan, 39(2):269–286, 1987.

[Mom95] Fumiyuki Momose.
Isogenies of prime degree over number fields.
Compositio Mathematica, 97(3):329–348, 1995.

[ÖS19] Ekin Özman and Samir Siksek.
Quadratic points on modular curves.
Mathematics of Computation, 88(319):2461–2484, 2019.

[Özm12] Ekin Özman.
Points on quadratic twists of $X_0(N)$.
Acta Arithmetica, 152:323–348, 2012.

[Yoo21] Hwajong Yoo.
The rational torsion subgroup of $J_0(N)$.
Preprint available online at https://arxiv.org/abs/2106.01020, 2021.