Towards strong uniformity for isogenies of prime degree

arxiv.org/abs/2302.08350 (submitted)

Barinder S. Banwait, Maarten Derickx

Boston University

Rational Points on Modular Curves
Thursday 21st September 2023
ICTS Bangalore, India

Torsion

Mordell-Weil Theorem

Theorem (Mordell (1922), Weil (1928))

Let E be an elliptic curve over a number field k. Then the group $E(k)$ of k-rational points on E is a finitely generated abelian group ; i.e.

$$E(k) \cong E(k)_{tors} \oplus \mathbb{Z}^r$$

for some $r \geq 0$.

Louis J. Mordell

André Weil

Question (Uniformity for torsion)

What possible groups can arise as $E(k)_{tors}$?

Question (Uniformity for torsion)

(For a fixed k), what possible groups can arise as $E(k)_{tors}$ (as E varies over all elliptic curves over k)?

Question (Strong uniformity for torsion)

For a fixed $d \geq 1$, what possible groups can arise as $E(k)_{tors}$ as k varies over all number fields of degree d over $\mathbb{Q}$ and E varies over all elliptic curves over k?

Let's call this set of possible groups $\Phi(d)$.

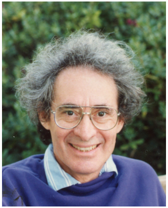
Mazur's Torsion Theorem

Theorem (Mazur, 1977)

$E(\mathbb{Q})_{tors}$ is one of the following 15 groups:

$$\begin{aligned} \mathbb{Z}/N\mathbb{Z}, &\qquad 1 \le N \le 10 \text{ or } N = 12 \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2N\mathbb{Z}, &\qquad 1 \le N \le 4. \end{aligned}$$

Moreover, each group occurs infinitely often.



Barry C. Mazur

This was conjectured by Beppo Levi in 1908 (in his Rome ICM address), then again by Andrew Ogg in 1970.

Actually, Mazur *really* proves the following result.

Theorem (Mazur (1977))

Let E be an elliptic curve over $\mathbb{Q}$ admitting a $\mathbb{Q}$-rational torsion point of prime order p. Then

$$p \in \{2, 3, 5, 7\}.$$

First reduction. — *To prove* (5.1-3) *it suffices to prove* (5.2) *in the special case where* $m = \mathrm{N}$, *a prime number such that the genus of* $\mathrm{X}_0(\mathrm{N})$ *is* >0 (*i.e.* $\mathrm{N} \neq 2, 3, 5, 7$, *and* 13).

This is so by virtue of the close study of the above conjecture of Ogg, made by Kubert, for low values of composite numbers m.

In particular, Kubert has shown ([27], chap. IV) that it suffices to consider only prime values of m, greater than or equal to 23. For $m = 13$, see [40].

SLOGAN

For $d = 1$ strong uniformity for torsion boils down to bounding torsion primes in degree d.

Kamienny-Mazur reduction

Rational Torsion of Prime Order in Elliptic Curves over Number Fields

S. Kamienny and B. Mazur
(with an appendix by A. Granville)

Definition. *Let d be a positive integer. A prime number p will be called a* **torsion prime for degree** *d if there is a number field k of degree d, an elliptic curve E defined over k, and a k-rational point P of E, of order p.*

Denote by $S(d)$ the set of torsion primes of degree $\leq d$. It has long been conjectured that $S(d)$ is finite for every d.

Proposition. *$S(d)$ is finite if and only if $\Phi(d)$ is finite.*

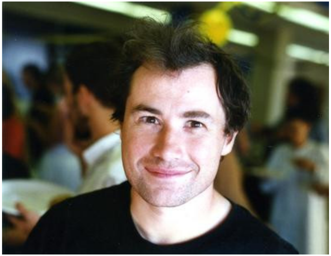
One should note, however, that even if $S(d)$ is given explicitly, the proposition will *not* provide an effective determination of $\Phi(d)$.

Proof of the Proposition. Clearly, if $\Phi(d)$ is finite, then so is $S(d)$. Suppose, then, that $S(d)$ is finite.

The set $\Phi(d)$ will be shown to be finite provided that we can bound, for

Merel's theorem (1996)

Théorème. *Soit* E *une courbe elliptique, définie sur un corps de nombres* K *de degré* $d > 1$ *sur* $\mathbf{Q}$. *Si* E(K) *possède un point d'ordre premier* p, *on a* $p < d^{3d^2}$.



Loïc Merel

The bound was subsequently improved to $(1 + 3^{d/2})^2$ by Oesterlé also in 1996 (unpublished, but appeared as an appendix to Derickx's PhD thesis).

Theorem (the people shown below (1977-2023))

$$S(1) = \{2,3,5,7\}$$
$$S(2) = \{2,3,5,7,11,13\}$$
$$S(3) = \{2,3,5,7,11,13\}$$
$$S(4) = \{2,3,5,7,11,13,17\}$$
$$S(5) = \{2,3,5,7,11,13,17,19\}$$
$$S(6) = \{2,3,5,7,11,13,17,19,37\}$$
$$S(7) = \{2,3,5,7,11,13,17,19,23\}$$
$$S(8) = \{2,3,5,7,11,13,17,19,23\}$$

Derickx

Kamienny

Khawaja

Mazur

Parent

Stein

Stoll

$\Phi(1)$, $\Phi(2)$ and $\Phi(3)$

Theorem (Mazur (1977))

$\Phi(1)$ *consists of the following* 15 *groups:*

$$\begin{array}{ll} \mathbb{Z}/m\mathbb{Z}, & \text{for } 1 \leq m \leq 12,\ m \neq 11, \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2m\mathbb{Z}, & \text{for } 1 \leq m \leq 4. \end{array}$$

Theorem (Kamienny-Kenku-Momose (1992))

$\Phi(2)$ *consists of the following* 26 *groups:*

$$\begin{array}{ll} \mathbb{Z}/m\mathbb{Z}, & \text{for } 1 \leq m \leq 18,\ m \neq 17, \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2m\mathbb{Z}, & \text{for } 1 \leq m \leq 6, \\ \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3m\mathbb{Z}, & \text{for } 1 \leq m \leq 2, \\ \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}. & \end{array}$$

Theorem (Derickx–Etropolski–van Hoeij–Morrow–Zureick-Brown (2021))

$\Phi(3)$ *consists of the following* 26 *groups:*

$$\begin{array}{ll} \mathbb{Z}/m\mathbb{Z}, & \text{for } 1 \leq m \leq 21,\ m \neq 17, 19 \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2m\mathbb{Z}, & \text{for } 1 \leq m \leq 7. \end{array}$$

Uniformity vs strong uniformity

Question (Strong uniformity for torsion)

For a fixed $d \geq 1$, what possible groups can arise as $E(k)_{tors}$ as k varies over all number fields of degree d over $\mathbb{Q}$ and E varies over all elliptic curves over k?

Question (Uniformity for torsion)

(For a fixed k), what possible groups can arise as $E(k)_{tors}$ (as E varies over all elliptic curves over k)?

Theorem (Najman (2011))

1. *Let E be an elliptic curve over $K = \mathbb{Q}(\sqrt{-3})$. Then $E(K)_{tors}$ is isomorphic to one of the groups in Mazur's list,* $\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$, $\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}$, $\mathbb{Z}/13\mathbb{Z}$ *or* $\mathbb{Z}/18\mathbb{Z}$.
2. *Let E be an elliptic curve over $K = \mathbb{Q}(i)$. Then $E(K)_{tors}$ is isomorphic to one of the groups in Mazur's list,* $\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$, *or* $\mathbb{Z}/13\mathbb{Z}$.

Filip Najman

Later today in Zagreb ...

Theorem (B.-Derickx, 2023)

For $K = \mathbb{Q}(\sqrt{d})$, $|d| < 500$, we determine which torsion subgroups arise over K.

Isogenies

If $P \in E(k)_{tors}$ of order p, then $\langle P \rangle$ is a G_K-stable subgroup of order p ; i.e., it gives rise to a k-rational p-isogeny.

Question (Uniformity for 'isogeny primes')

Fox a fixed k, what possible primes arise as the degree of a k-rational isogeny (as E varies over all elliptic curves over k)? Call this set IsogPrimeDeg(k).

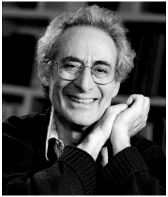
Question (Strong uniformity for isogeny primes)

Fox a fixed $d \geq 1$, what possible primes arise as the degree of a k-rational isogeny (as k varies over all number fields of degree d over $\mathbb{Q}$ and E varies over all elliptic curves over k)?

Mazur's isogeny theorem

Theorem (Mazur (1978))

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



Barry C. Mazur

Question (John Cremona to me (2010))

Mazur found $\mathrm{IsogPrimeDeg}(\mathbb{Q})$ *in 1978, can you do it for any other number field?*

Beware CM ...

If E/k has CM by $\mathcal{O}$ that is defined over k, i.e.

$$\mathrm{End}_K(E) = \mathcal{O},$$

then any prime p that splits in $\mathcal{O}$ will correspond to a k-rational endomorphism of degree p.

Lemma

If k contains the HCF of an IQF, then $\mathrm{IsogPrimeDeg}(k)$ *is infinite.*

Theorem (Momose (1995) + Merel (1996))

Assuming GRH, the converse of the above is true.

Question

Assume GRH. Let k be a number field not containing HCF of IQF. What is the finite set $\mathrm{IsogPrimeDeg}(k)$*?*

Uniformity for isogeny primes for some quadratic k

Theorem (B. (2021))

Assuming GRH, we have the following.

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

Uniformity for isogeny primes for some cubic k

Theorem (B.-Derickx (2022))

Assuming GRH, we have the following:

$$\begin{aligned}\mathrm{IsogPrimeDeg}(\mathbb{Q}(\zeta_7)^+) &= \mathrm{IsogPrimeDeg}(\mathbb{Q})\\ \mathrm{IsogPrimeDeg}(\mathbb{Q}(\alpha)) &= \mathrm{IsogPrimeDeg}(\mathbb{Q}) \cup \{29\}\\ \mathrm{IsogPrimeDeg}(\mathbb{Q}(\beta)) &= \mathrm{IsogPrimeDeg}(\mathbb{Q}),\end{aligned}$$

where $\alpha^3 - \alpha^2 - 2\alpha - 20 = 0$ *and* $\beta^3 - \beta^2 - 3\beta + 1 = 0$.

Selfie with Maarten Derickx in West London in January 2022

What about strong uniformity of isogenies?

Strong uniformity of isogenies can't be true in general because of the aforementioned CM isogenies.

Open Problem (Strong uniformity of isogenies v2)

For a fixed $d \geq 1$, what possible primes arise as the degree of a non-CM-over-k k-rational isogeny (as k and E vary as before)?

Note that if d is odd, then this "non-CM-over-k" can be removed.
Pete Clark calls this question *Isogeny Merel*, since it now has a hope of being a finite set, and one can ask about a bound on it in terms only of d.

Our main theorem (rough version)

Theorem (B.-Derickx (2023))

We establish Isogeny Merel for isogenies whose signature satisfies one of various conditions.

The signature of an isogeny

The name was coined by Nuno Freitas and Samir Siksek in 2013

As K is Galois, G acts transitively of $\mathfrak{p} \mid p$. Fix $\mathfrak{p}_0 \mid p$. For each $\tau \in G$ write s_τ for the number $s_\mathfrak{p}$ associated to the ideal $\mathfrak{p} := \tau^{-1}(\mathfrak{p}_0)$ by the previous proposition. We shall refer to $\mathbf{s} := (s_\tau)_{\tau \in G}$ as the **isogeny signature** of E at p. The set $S := \{0, 12\}^G$ shall denote the set of all possible sequences of values 0, 12 indexed

and it expresses information about the isogeny character.

Isogeny Character

Definition

Let E/k be an elliptic curve over a number field admitting a k-rational p-isogeny. The isogeny character is the character expressing the Galois action on the kernel W of the isogeny:

$$\lambda : G_k \to \mathrm{Aut}(W(\bar{k})) \cong \mathbb{F}_p^\times.$$

Since it is a one-dimensional Galois character it corresponds to an abelian extension of k, so precomposing with the Artin map we may identify λ with a character

$$I_k(p) \to \mathbb{F}_p^\times$$

on the group of fractional ideals of k coprime to p. By abuse of notation we also call this λ.

Key Proposition

The following key result expresses how λ^{12} acts on principal ideals:

Proposition

Let k be a number field, K its Galois closure, $\Sigma = Hom(k, K)$, and λ a p-isogeny character over k. Then for every prime ideal $\mathfrak{p}_0$ lying above p in K there exists a formal sum $\varepsilon = \varepsilon_{\mathfrak{p}_0} = \sum_{\sigma\in\Sigma} a_\sigma \sigma$ with all $a_\sigma \in \{0, 4, 6, 8, 12\}$ such that for all $\alpha \in k^\times$ prime to p,

$$\lambda^{12}((\alpha)) \equiv \alpha^{\varepsilon} \pmod{\mathfrak{p}_0}.$$

Furthermore if $p > 13$ and p is unramified in k, then for every $\mathfrak{p}_0$ there is a unique such signature $\varepsilon_{\mathfrak{p}_0}$.

This was first proven by Momose in 1995 under various conditions ($k = K$ and p unramified in k); a more careful treatment of it was given by David in 2009; in our previous work we remove these restrictions.

The isogeny signature

Definition

We refer to $\varepsilon_{\mathfrak{p}_0}$ as the isogeny signature of λ w.r.t. $\mathfrak{p}_0$.

- Different choice of $\mathfrak{p}_0$ permutes the a_σ integers (so we drop it from the notation);
- Fixing an ordering to Σ allows us to regard ε as a d-tuple of integers valued in $\{0, 4, 6, 8, 12\}$
- Really one first defines $a_\mathfrak{p}$ for $\mathfrak{p}$ a prime ideal of k; this has the interpretation that $\lambda^{12}|_{I_\mathfrak{p}} = \chi_p^{a_\mathfrak{p}}$; then one defines a_τ to be $a_\mathfrak{p}$ corresponding to $\mathfrak{p} = \tau^{-1}(\mathfrak{p}_0)$.
- In particular, if a_τ are all zero, then λ^{12} is an everywhere unramified character.

Summary

- It is a d-tuple of integers valued in $\{0, 4, 6, 8, 12\}$;
- Hence there are only 5^d of them ...
- ... but this depends on a choice of ordering of $\mathrm{Hom}(k, K)$.
- It expresses how inertia at p acts on the kernel of the isogeny;
- Isogeny Merel reduces to dealing with each possible signature.

Some special signatures

Definition

- If $\varepsilon = (0, \ldots, 0)$ or $(12, \ldots, 12)$, we say that ε is of Type 1.
- If $\varepsilon = (6, \ldots, 6)$ we say that ε is of Type 2.
- Define the trace of ε as $\operatorname{Tr} \varepsilon := \sum a_\sigma$.

Observe that $\operatorname{Tr} \varepsilon$ must satisfy one of:

- $\operatorname{Tr} \varepsilon \not\equiv 0 \pmod 6$ - $\checkmark$
- $\operatorname{Tr} \varepsilon \equiv 6 \pmod{12}$ - $\checkmark$assuming GRH
- $\operatorname{Tr} \varepsilon \equiv 0 \pmod{12}$ - only if ε is Type 1; otherwise this is OPEN

Results

The key proposition implies the following:

Proposition

Let λ be a p-isogeny character over k of signature ε and $\alpha \in k^\times$ coprime to p. Suppose the fractional ideal (α) factors as $\prod_{i=1}^r \mathfrak{q}_i^{e_i}$. Then for each $1 \le i \le r$ there exists

$$\beta_i \in S(\mathrm{Nm}(\mathfrak{q}_i), \overline{k}) := \{\pm 1, \pm \mathrm{Nm}(\mathfrak{q}_i)\} \cup \left\{\beta \in \overline{k} \mid \beta \text{ is a Frobenius root over } \mathbb{F}_{\mathfrak{q}_i}\right\},$$

and a prime ideal $\mathfrak{p}_i$ of $\mathbb{Q}(\beta_i)$ such that

$$\lambda(\mathrm{Frob}_{\mathfrak{q}_i}) \equiv \beta_i \pmod{\mathfrak{p}_i};$$

moreover one has that p divides the integer

$$B_{\varepsilon,\alpha,\beta} := \mathrm{Nm}_{\mathbb{Q}(\alpha^\varepsilon, \beta_1, \ldots, \beta_r)/\mathbb{Q}} \left(\alpha^\varepsilon - \prod_{i=1}^r \beta_i^{12 e_i} \right).$$

We apply this for $\alpha = q$ a rational integer; we loop over all possible splittings of (q) in a degree d number field, and take the lcm of the resulting $B_{\varepsilon,\alpha,\beta}$ integers to remove the dependence on k.

Algorithm 4.1

Algorithm 4.1. *Given the following inputs:*

- *an integer* $d \geq 1$;
- *a* d*-tuple* $\varepsilon \in \{0, 4, 6, 8, 12\}^d$;
- *a rational prime* q,

compute two integers $B_{\varepsilon,q}$ *and* $B^*_{\varepsilon,q}$ *as follows.*

```
def B_eps_q(d, eps, q, known_mult_bound=0):

    split_types = splitting_types(d)
    B_star = 1
    B = 1
    for split_type in split_types:
        pil_int_star, pil_int = bound_from_split_type(split_type, eps, q, known_mult_bound)
        B_star = gcd(known_mult_bound, lcm(B_star, pil_int_star))
        B = gcd(known_mult_bound, lcm(B, pil_int))
    return B_star, B
```

SLOGAN

$B_{\varepsilon,q}$ is a multiplicative bound on isogeny primes of signature ε, but it might be zero :(

$\operatorname{Tr} \varepsilon \not\equiv 0 \pmod{6}$

Proposition

If $\operatorname{Tr}(\varepsilon) \not\equiv 0 \pmod{6}$*, then none of the* $B_{\varepsilon,\boldsymbol{q},\beta}$ *are zero.*

Proof.

If $B_{\varepsilon,\boldsymbol{q},\beta} = 0$ for some β,then

$$q^{\operatorname{Tr} \varepsilon} = \prod_{i=1}^{r} \beta_i^{12e_i}.$$

By considering the absolute value of this equation, and observing that the only possible values for $|\beta_i|$ are 1, $\sqrt{q}^{f_i}$, or q^{f_i}, we see that 6 must divide $\operatorname{Tr} \varepsilon$. $\square$

Theorem (B.-Derickx)

Let k be a number field of degree d, and E/k an elliptic curve admitting a k-rational p-isogeny of signature ε for p prime. Assume $\mathrm{Tr}\,\varepsilon \not\equiv 0 \pmod 6$. Then for all primes q, we have $B_{\varepsilon,q} \neq 0$, $p | B_{\varepsilon,q}$, and

$$p \leq (2^{\mathrm{Tr}\,\varepsilon} + 2^{12d})^{2^d}.$$

$\operatorname{Tr}\varepsilon \equiv 6 \pmod{12}$ (Sketch)

Here one can show that $B_{\varepsilon,q} = 0$, and that if $p \nmid B^*_{\varepsilon,q}$, then p splits in $\mathbb{Q}(\sqrt{-q})$.
Using Effective Chebotarev, we can find a q for which p does not split in $\mathbb{Q}(\sqrt{-q})$ that satisfies

$$q \leq (4\log p + 10)^2;$$

for this q, we then have that $p | B^*_{\varepsilon,q}$ and hence

$$p \leq (q^{\operatorname{Tr}\varepsilon} + q^{12d})^{2^d};$$

these two inequalities contradict each other for large p.

Theorem (B.-Derickx)

Let k be a number field of degree d, and E/k an elliptic curve admitting a k-rational p-isogeny of signature ε for p prime. Assume $\operatorname{Tr}\varepsilon \equiv 6 \pmod{12}$, *and assume GRH. Then*

$$p \le \max\left(\left(10^{9\operatorname{Tr}\varepsilon} + 10^{108d}\right)^{2^d}, R_d\right),$$

where R_d is the largest real root of the function

$$x - \left(g(x)^{2\operatorname{Tr}\varepsilon} + g(x)^{24d}\right)^{2^d}$$

and $g(x) = \log(6x) + 9 + \frac{5}{2}(\log\log(6x))^2$.

ε is of Type 1

WLOG $\varepsilon = (0, \ldots, 0)$. If one of the $B_{\varepsilon,q,\beta} = 0$, then

$$\prod_{i=1}^{r} \beta_i^{12e_i} = 1$$

for some splitting type $(r, e_1, \ldots, e_r, f_1, \ldots, f_r)$. The only way this can happen is if all of the β_i are equal to ± 1 (because the Frobenius roots here have norm a power of q);in particular

$$\lambda^2(\mathrm{Frob}_{\mathfrak{q}_i}) \equiv 1 \pmod{p}.$$

If E had potentially good reduction at some $\mathfrak{q}_i$, then we'd get a nontrivial multiplicative bound ; so we can assume that E has potentially multiplicative reduction at all $\mathfrak{q}_i$. Writing x for the corresponding k-point on $X_0(p)$, this means that x specializes to one of the cusps 0 of ∞ at $\mathfrak{q}_i$. If x reduced to 0 at some $\mathfrak{q}_i$, then

$$\lambda^2(\mathrm{Frob}_{\mathfrak{q}_i}) \equiv \mathrm{Nm}(\mathfrak{q}_i)^2 \pmod{p},$$

and hence $p | (\mathrm{Nm}(\mathfrak{q}_i)^2 - 1)$. Otherwise, x reduces to ∞ at all $\mathfrak{q}_i$. This is then precisely the Kamienny-Mazur formal immersion setup, and hence (applying DKSS) p divides BadFormalImmersion(d).

Theorem (B.-Derickx)

Let k be a number field of degree d, E/k an elliptic curve admitting a k-rational p-isogeny of signature ε of type 1, and $q \geq 3$ a rational prime. Then p divides the nonzero integer

$$\operatorname{lcm}\left(B^*_{\varepsilon,q}, \prod_{f=1}^{d}(q^f - 1), \mathrm{BadFormalImmersion}(d), \mathrm{AGFI}_d(q)\right),$$

and in particular,

$$p \leq \max\left(65(2d)^6, (3^{12d} + 1)^{2^d}\right).$$

Strong uniformity of torsion in unramified extensions

Corollary

Let $d \geq 1$ be an integer, and let E be an elliptic curve over a number field k of degree d. If E attains a torsion point of prime order p rational over an extension of k that is unramified at all primes of k above p, then

$$p \leq \max\left(65(2d)^6, (3^{12d}+1)^{2^d}\right).$$

This generalises Merel's theorem (which is the case of the trivial extension of k).

Proof.

Let L be the extension in the statement, and P the torsion point. WLOG L/k is Galois. If $\langle P \rangle$ is k-rational, then E has a k-rational p-isogeny which is of Type 1 (by assumption of L being unramified above p) so the previous bound applies. If $\langle P \rangle$ is not k-rational, then P and $\sigma(P)$ generate $E[p]$ for some $\sigma \in \mathrm{Gal}(L/k)$; this implies $\zeta_p \in L$, so considering ramificiation, we get $p - 1 < d$; in both cases p is bounded by the previous bound. □

An exact list for Type 1 isogenies if $d = 2$

Theorem (B.-Derickx)

Let k be a number field of degree d, E/k an elliptic curve admitting a k-rational p-isogeny of signature ε of type 1, and $q \geq 3$ a rational prime. Then p divides the nonzero integer

$$\operatorname{lcm}\left(B^*_{\varepsilon,q}, \prod_{f=1}^{d}(q^f - 1), \mathrm{BadFormalImmersion}(d), \mathrm{AGFI}_d(q)\right),$$

and in particular,

$$p \leq \max\left(65(2d)^6, (3^{12d} + 1)^{2^d}\right).$$

Theorem (B.-Derickx)

There exists an elliptic curve over a quadratic field K admitting a K-rational p-isogeny of signature $(0,0)$, for p prime, if and only if p is in the following set:

$$\{2, 3, 5, 7, 11, 13, 17, 19, 37, 43, 73\}.$$

$d = 2$

Demo of code