Article:
Khawaja, M. (2024) Torsion primes for elliptic curves over degree 8 number fields. Research in Number Theory, 10. 48. ISSN 2363-9555

https://doi.org/10.1007/s40993-024-00533-6

Research in Number Theory

RESEARCH

Torsion primes for elliptic curves over degree 8 number fields

Maleeha Khawaja

*Correspondence:
mkhawaja2@sheffield.ac.uk
School of Mathematics and Statistics, University of Sheffield, Hicks Building, Sheffield S3 7RH, UK

Data sharing is not applicable to this article as no datasets were generated or analysed during the current study

Abstract

Let $d \geq 1$ be an integer and let p be a rational prime. Recall that p is a torsion prime of degree d if there exists an elliptic curve E over a degree d number field K such that E has a K-rational point of order p. Derickx et al. (Algebra Number Theory 17(2):267–308, 2023) have computed the torsion primes of degrees 4, 5, 6 and 7. We verify that the techniques used in Derickx et al. (Algebra Number Theory 17(2):267–308, 2023) can be extended to determine the torsion primes of degree 8.

Keywords: Modular curves, Elliptic curves, Rational points, Abelian varieties

Mathematics Subject Classification: 11G05, 14G05, 14G25, 14H52

1 Introduction

Let $d \geq 1$ be an integer and let p be a rational prime. Recall that p is a **torsion prime of degree** d if there is a number field K of degree d and an elliptic curve E over K with a K-rational point of order p. Let $S(d)$ denote the set of torsion primes of degree d. Let Primes(x) denote the set of primes less or equal than x. Mazur [10,11] was the first to completely determine the set $S(d)$ for any integer d. He found that $S(1) = \text{Primes}(7)$. Kamienny [8] and Parent [13,14] determined the torsion primes of degrees 2 and 3, respectively, finding that $S(2) = S(3) = \text{Primes}(13)$. Building on the techniques used in these works, Derickx et al. [5] proved the following result.

Theorem 1.1 (Derickx, Kamienny, Stein and Stoll) *For an integer $d \geq 1$, let $S(d)$ be the set of torsion primes of degree d. Then,*

$$S(4) = \text{Primes}(17),\ S(5) = \text{Primes}(19), S(6) = \text{Primes}(19) \cup \{37\},\ \textit{and}\ S(7) = \text{Primes}(23).$$

We use the techniques and computations of the aforementioned paper to determine the set of torsion primes of degree 8.

Theorem 1.2 *For an integer $d \geq 1$, let $S(d)$ be the set defined above. Then,*

$$S(8) = \text{Primes}(23).$$

Although the study of low degree points on curves has received much attention in and of itself, the precise determination of the set of torsion primes of low degree has also had

several applications to the explicit resolution of Diophantine equations; see e.g. [1,7,9]. We expect Theorem 1.2 to have Diophantine applications in a similar manner.

The purpose of this note is to provide a proof of Theorem 1.2. We stress that none of the ideas or techniques used in this note are due to us and we are merely verifying that the techniques used to prove Theorem 1.1 can be extended to prove Theorem 1.2.

All computations were performed in `Magma` [2] using Stoll's code [15]. All supporting computations can be found at

https://github.com/MaleehaKhawaja/deg8torsionprimes.

After completing our computations we learnt that Maarten Derickx and Michael Stoll have independently determined the torsion primes of degree 8 in unpublished work, as well as computing smaller bounds for the sets $S(9)$ and $S(10)$.

The following two results form the theoretical basis of the proof. For the benefit of the reader, we include the proofs of these results here.

Let $d \geq 1$ be an integer over $\mathbb{Q}$. Let X be a curve over $\mathbb{Q}$, and let $X^{(d)}$ denote the d^{th} symmetric power of X. Recall that points in $X^{(d)}(\mathbb{Q})$ correspond to effective degree d divisors on X. Let $N \geq 1$ be an integer and suppose $X = X_1(N)$. Then $C_1(N)$ denotes the set of cusps on $X_1(N)$.

Lemma 1.1 (Derickx, Kamienny, Stein and Stoll) *Let $d \geq 1$ be an integer, and let p be a prime. Let α be defined by the following composition of maps*

$$\alpha : C_1(p)(\mathbb{Q})^d \to X_1(p)(\mathbb{Q})^d \to X_1(p)^{(d)}(\mathbb{Q}). \tag{1}$$

If α is surjective then $p \notin S(d)$.

Proof This is [5, Lemma 1.5]. Suppose, for a contradiction that $p \in S(d)$. Thus there is a non−cuspidal K−rational point on $X_1(p)$. Thus there is a pair (E, P) where E is an elliptic curve over K and P is a point of order p on K. Taking the sum of the Galois conjugates of P gives a rational effective degree d divisor on $X_1(p)$. This divisor isn't the sum of rational cusps - this contradicts the surjectivity of α. □

For a prime ℓ distinct from p, let red_ℓ denote the usual reduction map:

$$\mathrm{red}_\ell : X_1(p)^{(d)}(\mathbb{Q}) \to X_1(p)^{(d)}(\mathbb{F}_\ell).$$

Lemma 1.2 (Derickx, Kamienny, Stein and Stoll) *Let ℓ be a prime distinct from p. Let $\tilde{x} \in X_1(p)^{(d)}(\mathbb{F}_\ell)$. Suppose that the following two assumptions are satisfied.*

(a) *If $\tilde{x}$ is the sum of images of rational cusps under red_ℓ then the residue class of $\tilde{x}$ contains at most one rational point.*
(b) *If $\tilde{x}$ is not the sum of images of rational cusps under red_ℓ then the residue class of $\tilde{x}$ doesn't contain a rational point.*

Then $p \notin S(d)$.

Proof This is [5, Lemma 1.7]. We want to show that the map α, as defined in Lemma 1.1, is surjective. Let $x \in X_1(p)^{(d)}(\mathbb{Q})$ be a rational point in the residue class of $\bar{x}$. By taking the contrapositive of assumption (b), $\bar{x}$ is the sum of images of rational cusps under red_ℓ. That is

$$\bar{x} = \bar{x}_1 + ... + \bar{x}_d$$

where $\bar{x}_i = \mathrm{red}_\ell(x_i)$ for rational cusps $x_i \in X_1(p)^{(d)}(\mathbb{Q})$. Let

$$x' \coloneqq x_1 + ... + x_d \in X_1(p)^{(d)}(\mathbb{Q}).$$

Since x' is a rational point in the residue class of $\bar{x}$, it immediately follows from assumption (a) that $x = x'$. It follows that $x \in C_1(p)(\mathbb{Q})^d$ since $x = x'$ is the sum of rational cusps. By Lemma 1.1 we have $p \notin S(d)$. □

Since $\mathrm{Primes}(23) \subseteq S(8)$ (see [5, Proposition 1.3]), in order to prove Theorem 1.2, it remains to prove that the reverse inclusion holds. The smallest general bound for torsion primes of degree d is due to Oesterlé:

$$S(d) \subset \mathrm{Primes}((3^{d/2}+1)^2);$$

see [5, Sect. 6] for a proof. In particular we need to verify that both assumptions of Lemma 1.2 hold for $29 \leq p < 6724$. We say p is a **rank zero prime** if the Jacobian $J_1(p)$ of the modular curve $X_1(p)$ has rank 0 over $\mathbb{Q}$. In Sect. 2, we verify that Lemma 1.2 holds for all rank zero primes. In Sects. 3 and 4, we verify that assumptions (a) and (b) of Lemma 1.2 hold for all remaining primes.

2 Rank zero primes

We begin our verification at the primes p for which the Jacobian $J_1(p)$ of $X_1(p)$ has rank 0 over $\mathbb{Q}$. If p is such a prime then we refer to p as a **rank zero prime**. There are finitely many rank zero primes, and moreover p is a rank zero prime if and only if

$$p \leq 31 \qquad \text{or} \qquad p \in \{41, 47, 59, 71\};$$

see [3, Proposition 6.2.1].

Let X be a curve defined over $\mathbb{Q}$. Let $d \geq 1$ be an integer. Fix $x_0 \in X^{(d)}(\mathbb{Q})$. Let J be the Jacobian of X. Recall that the Abel–Jacobi map ι is given by

$$X^{(d)} \to J, \quad x \mapsto [x - x_0].$$

Recall that the $\mathbb{Q}$-**gonality** of X is the minimum degree of a map from X to $\mathbb{P}^1$ defined over $\mathbb{Q}$. We break the proof of [5, Corollary 3.5] into smaller parts.

Lemma 2.1 *Let $d \geq 1$ be an integer. Suppose p is a prime such the $\mathbb{Q}$-gonality of $X_1(p)$ is strictly greater than d. Then the map*

$$\iota : X_1(p)^{(d)}(\mathbb{Q}) \to J_1(p)(\mathbb{Q})$$

is injective.

Proof Suppose there exist $x_1, x_2 \in X_1(p)^{(d)}(\mathbb{Q})$ such that $\iota(x_1) = \iota(x_2)$. Then

$$x_1 - x_2 = D_1 - D_2 + (f), \qquad D_1, D_2 \in J_1(p)(\mathbb{Q}),\ f \in L(D_1 - D_2).$$

In particular, the degree of $f \in \mathbb{Q}(X_1(p))$ is less than or equal to d. This contradicts the assumption on the $\mathbb{Q}$-gonality of $X_1(p)$. □

Lemma 2.2 (Derickx, Kamienny, Stein and Stoll) *Let $d \geq 1$ be an integer. Suppose $p \geq 3$ is a rank zero prime such that the $\mathbb{Q}$-gonality of $X_1(p)$ is strictly greater than d. Then assumption (a) of Lemma 1.2 is satisfied for p with $\ell = 2$.*

Proof This is [5, Corollary 3.5]. We recall that we need to show that the reduction map $\mathrm{red}_2 : X_1(p)^{(d)}(\mathbb{Q}) \to X_1(p)^{(d)}(\mathbb{F}_2)$ is injective. It follows from Lemma 2.1 and [5, Proposition 3.4] that the map $\mathrm{red}_2 \circ \iota = \iota \circ \mathrm{red}_2$ is injective. Thus red_2 is injective. □

Let $p \in \{29, 31, 41, 47, 59, 71\}$. Then it follows from work of Derickx and van Hoeij [6] that the $\mathbb{Q}$-gonality of $X_1(p)$ is strictly greater than 8. Thus assumption (a) of Lemma 1.2 is satisfied with $\ell = 2$ by Lemma 2.2. We now verify that assumption (b) holds for these primes. One way to do this is to show that every $\bar{x} \in X_1(p)^{(d)}(\mathbb{F}_\ell)$ is the sum of images of rational cusps.

Lemma 2.3 *Let $p = 29$, 31 or 41. Then $p \notin S(8)$.*

Proof From the remarks above, it remains to demonstrate that assumption (b) of Lemma 1.2 is satisfied. We follow the proof of [5, Lemma 3.7]. Write $X = X_1(p)$ and $J = J_1(p)$. By [5, Corollary 3.3], $J(\mathbb{Q})$ is generated by the differences of rational cusps. Thus, if there is a rational point in the residue class of $\bar{x} \in X^{(8)}(\mathbb{F}_2)$ then $\bar{x}$ maps into the subgroup of $J(\mathbb{F}_2)$ that is generated by the differences of the images of the rational cusps. We use Stoll's code [15] to verify that, under the hypothesis of assumption (b), $\bar{x}$ doesn't map into this subgroup. The supporting computations can be found in the script `X129_31_41.m`. □

To verify that assumption (b) holds for the primes 47, 59, and 71, we shall need the following lemma.

Lemma 2.4 (Derickx) *Let $d \geq 1$ be an integer, and let $p \geq 3$ be a prime. Suppose $t \in \mathbb{T}$ kills the rational points on the Jacobian of $X_1(p)$ i.e.*

$$t(J_1(p)(\mathbb{Q})) = \{0\},$$

where $\mathbb{T}$ denotes the endomorphism ring of $J_1(p)$. Consider two points $\bar{x}_0, \bar{x} \in X_1(p)^{(d)}(\mathbb{F}_2)$ where $\bar{x}_0$ is a sum of images of rational cusps. If the divisor $t(\bar{x} - \bar{x}_0)$ is not principal then there is no rational point $x \in X_1(p)^{(d)}(\mathbb{Q})$ in the residue class of $\bar{x}$.

Proof This is [5, Lemma 8.6]. Let $X = X_1(p)$ and $J = J_1(p)$. Suppose there is a rational point $x \in X^{(d)}(\mathbb{Q})$ in the residue class of $\bar{x}$. Let $x_0 \in X^{(d)}(\mathbb{Q})$ be a point in the residue class of $\bar{x}_0$ that is the sum of rational cusps. By assumption, t sends points in $J(\mathbb{Q})$ to zero. Thus $t(x - x_0) = 0$ i.e. $t(x - x_0)$ is principal. In particular, it follows that $t(\bar{x} - \bar{x}_0)$ is principal. □

Lemma 2.5 *Let $p = 47$, 59 or 71. Then $p \notin S(8)$.*

Proof Let $p = 47$, 59 or 71. It remains to show that assumption (b) of Lemma 1.2 is satisfied. Let $X = X_1(p)$ and $J = J_1(p)$. Let x be a degree 8 point on $X = X_1(p)$ and write $\bar{x}$ for the corresponding divisor on $X_{\mathbb{F}_2}$. First consider $p = 47$. Using Stoll's code, we checked that there are no elliptic curves over $\mathbb{F}_{2^d}$ with a point of order $p = 47$ for $1 \leq d \leq 7$. Thus $\bar{x}$ is the sum of eight rational cusps. Recall that assumption (a) of Lemma 1.2 with $\ell = 2$ follows directly from Lemma 2.2. Thus x is the sum of eight rational cusps. This contradicts the assumption that x is a degree 8 point on $X = X_1(p)$. Now suppose $p = 59$ or 71. Write T_n for the n-th Hecke operator, and $\langle a \rangle$ for the diamond operator. Let $t = (\langle 3 \rangle - 1)(T_3 - 3\langle 3 \rangle - 1) \in \mathbb{T}$. We checked using `Magma` that the positive rank simple factors of $J_1(p)$ already occur in $J_0(p)$. Using Stoll's code, we checked that there are no elliptic curves over $\mathbb{F}_{2^d}$ with a point of order p for $1 \leq d \leq 6$. As before $\bar{x}$ can not be the sum of eight rational cusps. The only remaining possibility is that $\bar{x} = \bar{D} + \bar{y}$ where $\bar{D}$ is a degree 7 place on $X_{\mathbb{F}_2}$, and $\bar{y}$ is the reduction of a rational cusp. We note that $t(\bar{y})$ is principal, and $t(\bar{x})$ is principal. Hence $t(\bar{D})$ must be principal. Using Stoll's code we checked that for all degree 7 places $\bar{D}$ of $X_{\mathbb{F}_2}$, the divisor $t(\bar{D})$ is not principal, giving a contradiction in this case. All supporting computations can be found in the script `rankzeroprimes.m`. □

3 Verifying assumption (a)

Let ℓ and p be distinct primes. Suppose $\bar{x} \in X_1(p)^{(d)}(\mathbb{F}_\ell)$. We recall assumption (a) of Lemma 1.2: if $\bar{x}$ is the sum of images of rational cusps under red_ℓ then the residue class of $\bar{x}$ contains at most one rational point. Before stating the main strategy used to verify that this assumption holds, we state an important result that is used in the proof.

Theorem 3.1 [Derickx, Kamienny, Stein and Stoll] *Let $d \geq 1$ be an integer and let ℓ and p be distinct primes. Let $t : J_1(p) \to \mathcal{A}$ be a morphism of abelian schemes over $\mathbb{Z}_{(l)}$ such that:*

(i) *$t(J_1(p)(\mathbb{Q}))$ is finite;*
(ii) *$\ell > 2$ or $\#t(J_1(p)(\mathbb{Q}))$ is odd;*
(iii) *$t \circ \iota$ is a formal immersion at all $\bar{x} \in X_1(p)^{(d)}(\mathbb{F}_\ell)$ that are sums of images of rational cusps on $X_1(p)$.*

Then assumption (a) of Lemma 1.2 holds.

Proof This is [5, Corollary 4.3]. Suppose $x, x' \in X_1(p)^{(d)}(\mathbb{Q})$ are in the residue class of $\bar{x}$, where $\bar{x}$ is the sum of images of rational cusps. We want to show that $x = x'$. Let $y = (t \circ \iota)(x)$ and $y' = (t \circ \iota)(x')$. We note that y and y' lie in the same residue class, since x and x' do. It then follows from i) and ii) that $y = y'$. Under the hypothesis of assumption iii), a result of Parent [12, Lemma 4.13] asserts that the map

$$t \circ \iota : \mathrm{red}_\ell{}^{-1}(\bar{x}) \to \mathrm{red}_\ell{}^{-1}((t \circ \iota)(\bar{x}))$$

is an injection. Thus $x = x'$. □

We work with $\ell = 2$, and refer the reader to [5, Sect. 5] for the construction of an appropriate operator $t \in \mathbb{T}$. Indeed Derickx, Kamienny, Stein and Stoll [5, Corollary 5.2] prove that such a t satisfies assumptions (i) and (ii) of Theorem 3.1 with $\ell = 2$, and one can

apply Kamienny's criterion [5, Proposition 5.3] to verify assumption iii). We used Stoll's code to test whether Kamienny's criterion holds, and found that it holds for

$$137 < p < 6724, \quad p \neq 149, 157, 163, 193, 431. \tag{2}$$

This part of the verification required several parallel computations. The supporting code can be found in script `assumptiona.m`.

For the primes excluded by (2) we used Stoll's code to verify that assumption (a) holds by replacing $X_1(p)$ with an intermediate curve between $X_1(p)$ and $X_0(p)$, see [5, Corollary 4.4]; this criterion is similar to Theorem 3.1. The supporting code can be found in the script `remainingprimes.m`.

4 Verifying assumption (b)

Let p be a prime, and let ℓ be a prime distinct from p. Suppose $\bar{x} \in X_1(p)^{(d)}(\mathbb{F}_\ell)$. We recall assumption (b) of Lemma 1.2: if $\bar{x}$ isn't the sum of images of rational cusps under red_ℓ then the residue class of $\bar{x}$ doesn't contain a rational point. As remarked in [5, p. 272], to verify this assumption, it suffices to show that

(i) there is no elliptic curve E over $\mathbb{F}_{\ell^{d'}}$, for all $d' \leq d$, such that $p \mid \#E(\mathbb{F}_{\ell^{d'}})$;
(ii) $p \nmid \ell^{d'} \pm 1$ for all $d' \leq d$.

It immediately follows from a result of Waterhouse [16, Theorem 4.1] that

$$\#E(\mathbb{F}_{2^d}) \in \{r \in [\lceil (2^{d/2}-1)^2 \rceil, \lfloor (2^{d/2}+1)^2 \rfloor] \ : \ r \text{ is even}\} \cup \{r_d\}$$

where

$$r_d = \begin{cases} 2^d + m2^{d/2} + 1, \ m \in \{-2, -1, 0, 1, 2\} & \text{if d is even} \\ 2^d + m2^{(d+1)/2} + 1, \ m \in \{-1, 0, 1\} & \text{if d is odd.} \end{cases}$$

Thus it remains to show that assumption (b) holds for

$$p \in \{29, 31, 37, 41, 43, 47, 59, 61, 67, 71, \\ 73, 113, 127, 131, 137, 139, 241, 257\}.$$

By Lemma 2.3 and Lemma 2.5, we have $29, 31, 41, 47, 59, 71 \notin S(8)$. Thus, it remains to verify that assumption (b) holds for

$$p \in \{37, 43, 61, 67, 73, 113, 127, 131, 137, 139, 241, 257\}.$$

We fix some notation for the remainder of the paper. Let $X = X_1(p)$ and $J = J_1(p)$. Write T_n for the n-th Hecke operator, and $\langle a \rangle$ for the diamond operator. Let $t = (\langle 3 \rangle - 1)(T_3 - 3\langle 3 \rangle - 1) \in \mathbb{T}$. As shown in [5, pg. 303], the operator $T_3 - 3\langle 3 \rangle - 1$ kills rational torsion. For the relevant primes p, we verify that the operator $\langle 3 \rangle - 1$ maps J into an abelian subvariety of rank zero. Thus for such p the operator t kills $J(\mathbb{Q})$.

Lemma 4.1 *Let $p \in \{43, 61, 67, 73\}$. Then $p \notin S(8)$.*

Proof Suppose x is a degree 8 point on $X = X_1(p)$ and denote by $\bar{x}$ the corresponding divisor on $X_{\mathbb{F}_2}$. If $p = 61, 67$ or 73 then the operator $\langle 3 \rangle - 1$ maps $J = J_1(p)$ into an abelian

subvariety of rank zero by the proof of [5, Lemma 8.7]. If $p = 43$, we checked using `Magma` that that the positive-rank simple factors of $J_1(43)$ all occur in $J_0(43)$.

First suppose $p = 43, 61$ or 67. Using Stoll's code, we checked that there are no elliptic curves over $\mathbb{F}_{2^d}$ with a point of order p for $1 \leq d \leq 6$. Thus all places on $X_{\mathbb{F}_2}$ of those degrees d must be cuspidal. We proved that assumption (a) of Lemma 1.2 holds in Sect. 3. Then $\bar{x} = \bar{D} + \bar{y}$ where $\bar{D}$ is a degree 7 place on $X_{\mathbb{F}_2}$, and $\bar{y}$ is the reduction of a rational cusp. Since $t(\bar{x})$ and $t(\bar{y})$ are principal, it must be that $t(\bar{D})$ is principal. Using Stoll's code, we checked that $t(\bar{D})$ is not principal for all degree 7 places $\bar{D}$ on $X_{\mathbb{F}_2}$. This gives a contradiction.

Now suppose $p = 73$. Using Stoll's code, we checked that there are no elliptic curves over $\mathbb{F}_{2^d}$ with a point of order p for $1 \leq d \leq 5$. In each possible case, the support of $\bar{x}$ must contain a degree d place $\bar{D}$ such that $t(\bar{D})$ is principal where $d = 6, 7$ or 8. Again, we checked that $t(\bar{D})$ is not principal for all degree d places $\bar{D}$ on $X_{\mathbb{F}_2}$. The supporting computations can be found in the script `smallprimes.m`. □

Lemma 4.2 *Let $p \in \{113, 127, 131, 137, 139, 241, 257\}$. Then $p \notin S(8)$.*

Proof Let p be a prime as above. We follow the proof of [5, Corollary 7.2]. We checked using `Magma` that the positive rank simple factors of $J_1(p)$ already occur in $J_0(p)$. In order to apply [5, Proposition 7.1], it suffices to find a primitive root a modulo p. For $p \neq 131, 241$ we choose $a = 3$; for $p = 131$ we choose $a = 2$; for $p = 241$ we choose $a = 7$. Let $\mathrm{ord}(a)$ denote the order of a in $(\mathbb{Z}/p\mathbb{Z})^\times/\{\pm 1\}$. For each p we have $\mathrm{ord}(a) = (p-1)/2 > 3 \cdot 8$. We let $n = 7$ if $p \neq 131, 241$ and $n = 8$ otherwise. In all cases we check that the inequality

$$8 < \frac{325}{2^{16}} \cdot \frac{p^2 - 1}{n}$$

holds. Thus [5, Proposition 7.1] asserts that $p \notin S(8)$. The supporting `Magma` computations can be found in the script `largeprimes.m`. □

In order to complete the proof of Theorem 1.2, it remains to show that assumption (b) of Lemma 1.2 holds for $p = 37$.

Lemma 4.3 $37 \notin S(8)$.

Proof We follow closely the proofs of Lemmas 8.8 and 8.9 of [5]. We work with $\ell = 2$. Using Stoll's code, we checked that there are no elliptic curves over $\mathbb{F}_{2^d}$ with a point of order 37 for $d = 1, 2, 3, 4, 5, 8$. Thus all places on $X_{\mathbb{F}_2}$ of those degrees d must be cuspidal. The curve $X = X_1(37)$ has 18 rational cusps, and 18 irrational cusps; the latter are defined over $\mathbb{Q}(\zeta_{37})^+$. As 2 is inert in $\mathbb{Q}(\zeta_{37})^+$, the irrational cusps yield a single place on $X_{\mathbb{F}_2}$ of degree 18. Let x be a degree 8 point on $X = X_1(37)$, and write $\bar{x}$ for the corresponding divisor on $X_{\mathbb{F}_2}$. There are only three possible cases.

Case (I). $\bar{x}$ is the sum of eight rational cusps. We proved that assumption (a) of Lemma 1.2 holds in Sect. 3. Thus x is the sum of eight rational cusps giving a contradiction.

Case (II). $\bar{x} = \bar{D} + \bar{y}$ where $\bar{D}$ is a degree 7 place on $X_{\mathbb{F}_2}$, and $\bar{y}$ is the reduction of a rational cusp. We note that $t(\bar{y})$ is principal, and $t(\bar{x})$ is principal. Hence $t(\bar{D})$ must be principal. Using Stoll's code we checked that for all degree 7 places $\bar{D}$ of $X_{\mathbb{F}_2}$, the divisor $t(\bar{D})$ is not principal, giving a contradiction in this case.

Case (III). $\tilde{x} = \tilde{D} + \tilde{y} + \tilde{z}$ where $\tilde{D}$ is a place of degree 6 on $X_{\mathbb{F}_2}$ and $\tilde{y}, \tilde{z}$ are reductions of rational cusps, that may be distinct or equal. Again $t(\tilde{x})$, $t(\tilde{y})$ and $t(z)$ are principal, therefore $t(\tilde{D})$ must be principal. We checked using the same code that there is precisely one degree 6 place on $X_{\mathbb{F}_2}$ (up to the action of the diamond operators) such that $t(\tilde{D})$ is principal. As noted in [5], the divisor $\tilde{D}$ is the reduction of a degree 6 point D on X. To obtain a contradiction, it is enough to show that $D + y + z$ is the unique rational point on $X^{(8)}$ in the residue disk of $\tilde{D} + \tilde{y} + \tilde{z}$.

Continuing in the footsteps of [5, Lemma 8.8] we consider the projection $T_{17} : J \to A$, where A is a 36 dimensional abelian variety of rank 0, rational torsion subgroup of odd order; moreover the eigenvalues of T_{17} acting on the eigenforms coming from A are all odd. To show that $D + y + z$ is the unique rational point in the residue disk of $\tilde{D} + \tilde{y} + \tilde{z}$ it is enough to verify that the relevant 'Derickx matrix' (see [4, Proposition 3.7]) has rank 8. Using a basis for $S_2(\Gamma_1(37))$, which has dimension 40, Stoll's code constructs a canonical embedding for $X \subset \mathbb{P}^{39}$. Thus regular differentials on X may be identified with linear combinations of the coordinates on $\mathbb{P}^{39}$. With this identification, Stoll's code determines the differentials $\omega_1, \ldots, \omega_{36}$ coming from the rank zero quotient A. If the two cusps y, z are distinct, then the divisor $\tilde{D} + \tilde{y} + \tilde{z}$ is the sum of eight geometric points, say $\tilde{D} + \tilde{y} + \tilde{z} = \tilde{p}_1 + \cdots + \tilde{p}_8$. In this case, the Derickx matrix has a particularly simple form, $M = (\omega_i(p_j))$, and the formal immersion criterion is satisfied if this matrix has rank 8 (see [4, Proposition 3.7]). We do not know the degree 6 place $\tilde{D}$ on this particular model, but we checked, for all distinct pairs of rational cusps y, z, and all degree 6 places $\tilde{D}'$ on $X_{\mathbb{F}_2}$ that the matrix M for $\tilde{D}' + \tilde{y} + \tilde{z}$ has rank 8 as required.

It remains to consider the case where $y = z$. Note that the action of the diamond operators on the rational cusps is transitive, and one of these rational cusps is the ∞ cusp. Thus it is enough to show that the Derickx matrix for $\tilde{D}' + 2\infty$ has rank 8 for all degree 6 places on $X_{\mathbb{F}_2}$. Write $\tilde{D}' = p_1 + \cdots + p_6$ where the p_i are geometric points. Then the Derickx matrix is

$$M = \begin{pmatrix} \omega_1(p_1) & \omega_1(p_2) & \cdots & \omega_1(p_6) & a_1(\omega_1) & a_2(\omega_1) \\ \vdots & \vdots & & \vdots & \vdots & \vdots \\ \omega_{36}(p_1) & \omega_{36}(p_2) & \cdots & \omega_{36}(p_6) & a_1(\omega_{36}) & a_2(\omega_{36}) \end{pmatrix};$$

here $a_1(\omega)$ and $a_2(\omega)$ are the first two coefficients in the expansion of ω in terms of any uniformizer at ∞. Our differentials $\omega_1, \ldots, \omega_{36}$ come from cusp expansions around ∞, with the cusp expansion $f = a_1 q + a_2 q^2 + \cdots$ giving the differential $\omega = f(q)dq/q = (a_1 + a_2 q + \cdots)dq$. As q is a uniformizer for the ∞-cusp we may use these coefficients a_1, a_2 in the Derickx matrix. We computed all the possible matrices M and checked that they indeed have rank 8. This completes the proof. The supporting computations can be found in the script `X137.m`. □

Acknowledgements
The author is sincerely grateful to Frazer Jarvis and Michael Stoll for helpful correspondence, and would like to thank the anonymous referees for their invaluable feedback and careful reading of a previous version of the paper. The author is supported by an EPSRC studentship from the University of Sheffield (EP/T517835/1).

Data availability All supporting `Magma` computations can be found in the following public GitHub repository: https://github.com/MaleehaKhawaja/deg8torsionprimes.

Received: 24 May 2023 Accepted: 31 March 2024

Published online: 25 April 2024

References

1. Anni, S., Siksek, S.: Modular elliptic curves over real abelian fields and the generalized Fermat equation $x^{2\ell} + y^{2m} = z^p$. Algebra Number Theory **10**(6), 1147–1172 (2016)
2. Bosma, W., Cannon, J., Playoust, C.: The Magma algebra system. I. The user language. J. Symb. Comput. **24**, 235–265 (1997). Computational algebra and number theory (London, 1993)
3. Conrad, B., Edixhoven, B., Stein, W.: $J_1(p)$ has connected fibers. Doc. Math. **8**, 331–408 (2003)
4. Derickx, M.: Torsion points on elliptic curves over number fields of small degree. PhD thesis, Universiteit Leiden (2016)
5. Derickx, M., Kamienny, S., Stein, W., Stoll, M.: Torsion points on elliptic curves over number fields of small degree. Algebra Number Theory **17**(2), 267–308 (2023)
6. Derickx, M., van Hoeij, M.: Gonality of the modular curve $X_1(N)$. J. Algebra **417**, 52–71 (2014)
7. Freitas, N., Siksek, S.: Fermat's last theorem over some small real quadratic fields. Algebra Number Theory **9**(4), 875–895 (2015)
8. Kamienny, S.: Torsion points on elliptic curves and q-coefficients of modular forms. Invent. Math. **109**(2), 221–229 (1992)
9. Khawaja, M., Jarvis, F.: Fermat's last theorem over Q(p2,p3). arXiV Preprint (2022). https://arxiv.org/abs/2210.03744
10. Mazur, B.: Modular curves and the Eisenstein ideal. Inst. Hautes Études Sci. Publ. Math. **47**, 33–186 (1977). With an appendix by Mazur and M. Rapoport
11. Mazur, B.: Rational isogenies of prime degree (with an appendix by D. Goldfeld). Invent. Math. **44**(2), 129–162 (1978)
12. Parent, P.: Bornes effectives pour la torsion des courbes elliptiques sur les corps de nombres. J. Reine Angew. Math. **506**, 85–116 (1999)
13. Parent, P.: Torsion des courbes elliptiques sur les corps cubiques. Ann. Inst. Fourier (Grenoble) **50**(3), 723–749 (2000)
14. Parent, P.: No 17-torsion on elliptic curves over cubic number fields. J. Théor. Nombres Bordeaux **15**(3), 831–838 (2003)
15. Stoll, M.: Magma code for the paper 5 (2020). https://www.mathe2.uni-bayreuth.de/stoll/magma/index.html
16. Waterhouse, W.C.: Abelian varieties over finite fields. Ann. Sci. École Norm. Sup. **4**(2), 521–560 (1969)

Publisher's Note