ACTA ARITHMETICA
Online First version

Quadratic points on the Fermat quartic over number fields

by

Enrique González-Jiménez

Abstract. Let C be a curve defined over a number field K. A point $P \in C(\overline{\mathbb{Q}})$ is called K-quadratic if $[K(P):K]=2$. Let K be a number field such that the ranks of the elliptic curves $E_1 : y^2 = x^3+4x$ and $E_2 : y^2 = x^3-4x$ over K are 0. Under this condition, we prove that the set of K-quadratic points on the Fermat quartic $F_4\colon X^4+Y^4=Z^4$ is finite and computable and we provide a procedure to compute it. In particular, we explicitly compute all the K-quadratic points if $[K:\mathbb{Q}]<8$. Moreover, if the degree of K is odd, we prove that the K-quadratic points are just the $\mathbb{Q}$-quadratic points.

1. Introduction.

Fermat, in 1637, proved that the Fermat quartic $F_4\colon X^4+Y^4=Z^4$ has only trivial solutions (i.e. $XY=0$). Since then, numerous mathematicians have studied the solutions of this equation over number fields. Let K be a number field and denote by $F_4(K)$ the set of K-rational points of F_4. In this paper we aim to determine the set of K-quadratic points on F_4:

$$\Gamma_2(F_4,K) = \bigcup \{F_4(L) : K \subset L \subset \overline{\mathbb{Q}} \text{ and } [L:K]=2\}.$$

Aigner [2] gives $\Gamma_2(F_4,\mathbb{Q})$, proving that $\mathbb{Q}(\sqrt{-7})$ is the only quadratic extension that contains non-trivial solutions (note that $(1+\sqrt{-7})^4+(1-\sqrt{-7})^4 = 2^4$). Ishitsuka et al. [9, Theorem 7.3] give $\Gamma_2(F_4,\mathbb{Q}(\zeta_8))$, where ζ_8 is a primitive 8th root of unity. Recently, Tho [16], using a method of Mordell [12], has obtained a different proof from that of Ishitsuka et al. After completing this work, we became aware that Khawaja and Jarvis [10, §3 and Theorem 6.4] had previously studied the problem of determining the points on the Fermat quartic that lie in a quadratic extension of $\mathbb{Q}(\sqrt{2})$. In particular, they proved that all such points lie in one of the following fields: $\mathbb{Q}(\sqrt{2},\sqrt{-1})$, $\mathbb{Q}(\sqrt{2},\sqrt{-7})$, $\mathbb{Q}(\sqrt[4]{2})$, or $\mathbb{Q}(\sqrt{-1}\sqrt[4]{2})$. We have noted that the method used is essentially the same as the one employed by Tho [16], which serves as

---

2020 *Mathematics Subject Classification*: Primary 11D25; Secondary 14H52, 11G05, 14G05.
Key words and phrases: elliptic curve, Fermat quartic, quadratic point.
Received 25 April 2025.

DOI: 10.4064/aa250425-7-11

the basis of this article. Unlike previous articles, the present work uses the knowledge of the growth of the torsion of the elliptic curves $E_1 : y^2 = x^3+4x$ and $E_2 : y^2 = x^3 - 4x$ to obtain generalizations of the previous results.

In the present paper, we use Mordell's approach to provide a procedure for computing $\Gamma_2(F_4, K)$ in cases where the set is finite. In particular, if the degree of K is odd and $\Gamma_2(F_4, K)$ is a finite set, we prove that $\Gamma_2(F_4, K) = \Gamma_2(F_4, \mathbb{Q})$. Finally, we compute the finite set $\Gamma_2(F_4, K)$ explicitly if $[K : \mathbb{Q}] < 8$.

Note that if $\overline{\mathbb{Q}}$ denotes an algebraic closure of $\mathbb{Q}$, then $F_4(\overline{\mathbb{Q}})$ has the following *trivial points*:

$$\{[0 : \pm 1 : 1], [0 : \pm\zeta_8^2 : 1], [\pm 1 : 0 : 1], [\pm\zeta_8^2 : 0 : 1]\} \\ \cup \{[\zeta_8^j : 1 : 0], [1 : \zeta_8^j : 0] \,:\, j = 1, 3, 5, 7\}.$$

In particular,

$$[0 : \pm 1 : 1], [0 : \pm\zeta_8^2 : 1], [\pm 1 : 0 : 1], [\pm\zeta_8^2 : 0 : 1] \in \Gamma_2(F_4, \mathbb{Q}),$$

and

$$[1 : \zeta_8^j : 0] \in \Gamma_2(F_4, K) \quad \text{for } j = 1, 3, 5, 7,$$

if and only if $\mathbb{Q}(\sqrt{2}) \subset K$ or $\mathbb{Q}(\sqrt{-1}) \subset K$.

Suppose $Z \neq 0$. The change of variables $x = X/Z$ and $y = Y/Z$ gives the affine equation

$$F_4^0 \,:\, x^4 + y^4 = 1.$$

Note that if K is a number field and $(x, y) \in F_4^0(K)$, then the points $(\pm x, \pm y), (\pm y, \pm x)$ are in $F_4^0(K)$. We will say that $(x, y) \in F_4^0(K)$ is a *primitive point* of F_4^0 (or of F_4) if $(x, y) \notin F_4^0(K')$ for any proper subfield $K' \subset K$. Let us denote by $S_2^0(F_4, K)$ the set obtained from $\Gamma_2(F_4, K)$ after removing all trivial points, non-primitive points, and keeping only one representative (x, y) for each set $\{(\pm x, \pm y), (\pm y, \pm x)\}$.

Consider the elliptic curves

$$E_1 : y^2 = x^3 + 4x \quad \text{and} \quad E_2 : y^2 = x^3 - 4x.$$

The main result of this paper is the following:

THEOREM 1.1. *Let K be a number field such that* $\operatorname{rank}_{\mathbb{Z}} E_j(K) = 0$, $j = 1, 2$. *Then:*

(i) *$\Gamma_2(F_4, K)$ is finite and computable.*
(ii) *If $[K : \mathbb{Q}]$ is odd, then $\Gamma_2(F_4, K) = \Gamma_2(F_4, \mathbb{Q})$.*
(iii) *If $[K : \mathbb{Q}] < 8$, then $\Gamma_2(F_4, K) = \Gamma_2(F_4, L)$, where $L \in \{\mathbb{Q}, \mathbb{Q}(\sqrt{-1}), \mathbb{Q}(\sqrt{2}), \mathbb{Q}(\zeta_8), \mathbb{Q}(\alpha)\}$ (α satisfies $\alpha^4 - 2\alpha^2 - 1 = 0$) is the biggest number field such that $L \subseteq K$. Moreover, the set $S_2^0(F_4, L)$ appears in the following table:*

L	$S_2^0(F_4, L)$
$\mathbb{Q}$	$(\omega, \overline{\omega})$
$\mathbb{Q}(\sqrt{-1})$	$\sqrt{-1}(\omega, \overline{\omega}), \quad (\omega, \sqrt{-1}\overline{\omega}), \quad (\sqrt{-1}\omega, \overline{\omega})$
$\mathbb{Q}(\sqrt{2})$	$(1/\sqrt[4]{2}, 1/\sqrt[4]{2}), \quad \sqrt{-1}(1/\sqrt[4]{2}, 1/\sqrt[4]{2})$
$\mathbb{Q}(\alpha)$	$(\delta, -\alpha^3 + 2\alpha), \quad (\sqrt{-1}\delta, -\alpha^3 + 2\alpha)$
$\mathbb{Q}(\zeta_8)$	$(\zeta_8, \sqrt[4]{2}), \quad (\zeta_8^3, \sqrt[4]{2}), \quad \zeta_8(1, \zeta_8\sqrt[4]{2}), \quad \zeta_8^2(\zeta_8, \sqrt[4]{2}), \quad (1/\sqrt[4]{2}, \zeta_8^2/\sqrt[4]{2}),$ $\zeta_3\zeta_8(1, \zeta_3), \quad \zeta_3\zeta_8^3(1, \zeta_3), \quad \zeta_3\zeta_8(1, \zeta_3\zeta_8^2), \quad \zeta_3\zeta_8(\zeta_8^2, \zeta_3),$ $\omega^{-1}(\overline{\omega}\zeta_8, 1), \quad \omega^{-1}(\overline{\omega}\zeta_8^3, 1), \quad \omega^{-1}(\overline{\omega}\zeta_8, \zeta_8^2), \quad \omega^{-1}(\overline{\omega}\zeta_8^3, \zeta_8^2),$ $\overline{\omega}^{-1}(\omega\zeta_8, 1), \quad \overline{\omega}^{-1}(\omega\zeta_8^3, 1), \quad \overline{\omega}^{-1}(\omega\zeta_8, \zeta_8^2), \quad \overline{\omega}^{-1}(\omega\zeta_8^3, \zeta_8^2)$

where $\zeta_3 = e^{2i\pi/3}$, $\omega = (1 + \sqrt{-7})/2$, α *satisfies* $\alpha^4 - 2\alpha^2 - 1 = 0$ *and* δ *satisfies* $\delta^2 = \alpha^3 - 3\alpha$.

(iv) *Let* L *be a number field such that* $E_i(K) = E_i(L)$ *for* $i = 1, 2$. *Then* $\Gamma_2(F_4, K) = \Gamma_2(F_4, L)$.

The following corollaries are immediate consequences of the preceding theorem:

COROLLARY 1.2. *We have*

K	$\mathbb{Q}$	$\mathbb{Q}(\sqrt{-1})$	$\mathbb{Q}(\sqrt{2})$	$\mathbb{Q}(\alpha)$	$\mathbb{Q}(\zeta_8)$
$\lvert\Gamma_2(F_4, K)\rvert$	16	44	28	44	188

COROLLARY 1.3. *Let* K *be a number field. Then* F_4 *has non-trivial primitive points in a quadratic extension* L/K *in the following cases:*

(i) *If* $K = \mathbb{Q}$ *then* $L = \mathbb{Q}(\sqrt{-7})$.
(ii) *If* $K = \mathbb{Q}(\sqrt{-1})$ *then* $L = \mathbb{Q}(\sqrt{-1}, \sqrt{-7})$.
(iii) *If* $K = \mathbb{Q}(\sqrt{2})$ *then* $L = \mathbb{Q}(\sqrt[4]{2})$ *or* $L = \mathbb{Q}(\sqrt{-1}\sqrt[4]{2})$.
(iv) *If* $K = \mathbb{Q}(\alpha)$ *then* $L = \mathbb{Q}(\alpha, \sqrt{\alpha^3 - 3\alpha})$ *or* $L = \mathbb{Q}(\alpha, \sqrt{-\alpha^3 + 3\alpha})$.
(v) *If* $K = \mathbb{Q}(\zeta_8)$ *then* $L = \mathbb{Q}\left(\zeta_8, \sqrt[4]{2}\right)$, $L = \mathbb{Q}\left(\zeta_8, \sqrt{-3}\right)$, *or* $L = \mathbb{Q}\left(\zeta_8, \sqrt{-7}\right)$.

In particular, (i) is Aigner's result and (v) is Ishitsuka et al.'s result.

REMARK. A straightforward consequence of Theorem 1.1(iv) is that one can compute $\Gamma_2(F_4, K)$ for certain number fields K with $[K : \mathbb{Q}] > 8$. For instance, when $K = \mathbb{Q}(\zeta_{16})$, we have $\Gamma_2(F_4, \mathbb{Q}(\zeta_{16})) = \Gamma_2(F_4, \mathbb{Q}(\zeta_8))$, since $E_i(\mathbb{Q}(\zeta_{16})) = E_i(\mathbb{Q}(\zeta_8))$ for $i = 1, 2$.

This article is organized as follows. Section 2 is devoted to the study of quadratic points on a curve. In particular, we describe an algorithm that, in practice, computes $\Gamma_2(C, K)$ when the Jacobian of C has only finitely many K-rational points. In Section 3, we note that the Fermat quartic F_4 is isomorphic over $\mathbb{Q}$ to the modular curve $X_0(64)$, and we recall a method due to Ozman and Siksek [13] to determine $\Gamma_2(X_0(64),\mathbb{Q})$. Although this method is, in principle, difficult to apply when replacing $\mathbb{Q}$ with a number field K, we explain in Section 5 a technique inspired by an idea of Mordell that allows us to determine $\Gamma_2(X_0(64),K)$, provided that $E_1(K)$ and $E_2(K)$ are finite. Section 4 contains another notable result, Proposition 4.1, where we prove that if E is an elliptic curve defined over $\mathbb{Q}$ with $j(E) = 1728$, then the torsion subgroup $E(\mathbb{Q})_{\rm tors}$ does not grow in any number field of odd degree. This result is of independent interest beyond the context of quadratic points on the Fermat quartic, and it plays a key role in the proof of Theorem 1.1(ii). Finally, in Section 6, we provide the proof of the main result of the article, Theorem 1.1. The Appendix contains relevant data concerning certain genus 1 curves that are used throughout the article. We also list several number fields of degree less than 7 that satisfy the conditions in Theorem 1.1.

This work makes extensive use of the computer algebra system `Magma` [4]. The code verifying the computational claims made in this paper is available at [5].

2. Quadratic points on curves. One of the fundamental results in the theory of quadratic points on curves is the following, which follows from results by Abramovich and Harris [1] and Harris and Silverman [8] (see also [3]).

THEOREM 2.1. *Let C be a curve defined over a number field K of genus $g \geq 2$. Then $\Gamma_2(C,K)$ is an infinite set if and only if C is hyperelliptic over K or bielliptic over K with a bielliptic map $C \to E$ such that the elliptic curve E has positive rank over K.*

For a non-hyperelliptic curve C of genus ≥ 3 defined over a number field K with finite $J(K)$, where J is the Jacobian of C, and at least one point $P_0 \in C(K)$, a theoretical method exists to determine all quadratic points by computing effective degree 2 rational divisors. This relies on the injective map $\iota : C^{(2)}(K) \to J(K)$, where $C^{(2)}$ denote the second symmetric product of C, which enables the recovery of quadratic points from elements of $J(K)$. For each $[D] \in J(K)$, one computes the Riemann–Roch space $\mathcal{L}(D + 2P_0)$. If its dimension is 1, an effective divisor of degree 2 can be determined. However, computing $J(K)$ is often difficult. Even when feasible, the required Riemann–Roch computations may be impractical for large groups.

Thus, while theoretically sound, this approach is computationally demanding and may not always be practical.

In Section 5, we present a much simpler method than the previous one, based on Mordell's ideas, which allows us to determine the quadratic points of the Fermat quartic over a number field.

3. A modular approach. It is noteworthy that the Fermat quartic is $\mathbb{Q}$-isomorphic to the non-hyperelliptic genus 3 modular curve $X_0(64)$, and E_1 is $\mathbb{Q}$-isomorphic to the modular curve $X_0(32)$.

Ozman and Siksek [13] determine the quadratic points on the modular curves $X_0(N)$, where the curve is non-hyperelliptic, the genus is 3, 4 or 5, and the Mordell–Weil group of $J_0(N)$ is finite. In particular, this applies to the modular curve $X_0(64)$. Their method involves first determining the rational cuspidal subgroup $C_0(64)(\mathbb{Q})$ (see [13] for definition) and then bounding its index in $J_0(64)(\mathbb{Q})$, where $J_0(64)$ is the Jacobian of $X_0(64)$. This provides a positive integer I such that $I \cdot J_0(64)(\mathbb{Q}) \subseteq C_0(64)(\mathbb{Q})$. Consequently, the effective degree 2 divisors D satisfy $[D - 2P_0] = I \cdot [D']$ for some $[D'] \in J_0(64)(\mathbb{Q})$. To refine the search, they apply a version of the Mordell–Weil sieve to eliminate most possibilities for D'. Finally, they use Riemann–Roch theory to explicitly determine the divisors D.

It would seem natural to apply this method by replacing $\mathbb{Q}$ by a number field K which $J_0(64)(K)$ is finite. Although theoretically this seems possible, the calculations involved in number fields lead us to believe that achieving our goal would not be easy, assuming everything worked as expected. For this reason, we propose a much simpler method in Section 5 that works efficiently.

Lemma 3.1. *We have* $J_0(64) \overset{\mathbb{Q}}{\sim} E_1^2 \times E_2$. *In particular, if* K *is a number field, then* $\operatorname{rank}_{\mathbb{Z}} J_0(64)(K) = 2\operatorname{rank}_{\mathbb{Z}} E_1(K) + \operatorname{rank}_{\mathbb{Z}} E_2(K)$.

Proof. The following table shows, in the first column, three involutions in F_4 along with their corresponding definitions; the last column presents the quotient elliptic curve obtained from these involutions:

ϕ	$\phi([X:Y:Z])$	$F_4/\langle\phi\rangle$
ϕ_1	$[-X:Y:Z]$	E_1
ϕ_2	$[X:-Y:Z]$	E_1
ϕ_3	$[X:Y:-Z]$	E_2

Since the genus of $X_0(64)$ is 3, the above table shows

$$J_0(64) \overset{\mathbb{Q}}{\sim} E_1^2 \times E_2.$$

In particular, $\operatorname{rank}_{\mathbb{Z}} J_0(64)(K) = 2\operatorname{rank}_{\mathbb{Z}} E_1(K) + \operatorname{rank}_{\mathbb{Z}} E_2(K)$. ∎

4. On torsion growth of elliptic curves. The following result is of independent interest. It will directly lead to the deduction of the second part of Theorem 1.1.

PROPOSITION 4.1. *Let E be an elliptic curve defined over $\mathbb{Q}$ with $j(E) = 1728$ and K a number field of odd degree. Then $E(K)_{\text{tors}} = E(\mathbb{Q})_{\text{tors}}$.*

Proof. First of all, since $j(E) = 1728$, we note that E is $\mathbb{Q}$-isomorphic to $E_k : y^2 = x^3 + kx$ for some fourth-power-free integer k (see [15, Appendix A, §3]). It is well known that (see [14, Chap. X, Prop. 6.1(a)])

$$E_k(\mathbb{Q})_{\text{tors}} \simeq \begin{cases} \mathbb{Z}/4\mathbb{Z} & \text{if } k = 4, \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} & \text{if } -k \text{ is a perfect square,} \\ \mathbb{Z}/2\mathbb{Z} & \text{otherwise.} \end{cases}$$

Let us prove that if K is a number field such that $E(K)_{\text{tors}} \neq E(\mathbb{Q})_{\text{tors}}$, then its degree is even. To this end, it suffices to prove that if $P = (x, y) \in E(\overline{\mathbb{Q}})_{\text{tors}}$ with $P \notin E(\mathbb{Q})$, then $[\mathbb{Q}(P) : \mathbb{Q}]$ is even, where $\mathbb{Q}(P) = \mathbb{Q}(x, y)$. Specifically, it is sufficient to consider P of odd prime order p or of order a power of 2.

Let p be a prime and $G_E(p)$ be the image (up to conjugacy into $\mathrm{GL}_2(\mathbb{F}_p)$) of the mod p Galois representation on the p-torsion of E. In the complex multiplication case, the possibilities for $G_E(p)$ are completely understood, thanks to the work of Zywina [17, §1.9]. Since $j(E) = 1728$, E has complex multiplication by $\mathbb{Z}[\sqrt{-1}]$ and therefore

- if $p = 2$, then $G_E(p)$ is $B(2)$ or $\mathrm{C}_s(2)$,
- if $p \equiv 1 \pmod 4$, then $G_E(p)$ is $\mathrm{C}_{ns}^{+}(p)$ or $\mathrm{GL}_2(\mathbb{F}_p)$,
- if $p \equiv 3 \pmod 4$, then $G_E(p)$ is $\mathrm{C}_s^{+}(p)$ or $\mathrm{GL}_2(\mathbb{F}_p)$,

where $B(p)$ (resp. $\mathrm{C}_s(p)$, $\mathrm{C}_{ns}(p)$) denotes the Borel (resp. split Cartan, non-split Cartan) subgroup of $\mathrm{GL}_2(\mathbb{F}_p)$ and $\mathrm{C}_s^{+}(p)$ (resp. $\mathrm{C}_{ns}^{+}(p)$) is the normalizer of $\mathrm{C}_s(p)$ (resp. $\mathrm{C}_{ns}(p)$) in $\mathrm{GL}_2(\mathbb{F}_p)$.

Let p be a prime and let $P \in E[p]$ be a point of order p on the elliptic curve E. Then [6, Theorem 5.6] gives the possible degrees $[\mathbb{Q}(P) : \mathbb{Q}]$ depending on $G_E(p)$. In the particular case $j(E) = 1728$ we see that

- if $p = 2$, then $[\mathbb{Q}(P) : \mathbb{Q}] \in \{1, 2\}$,
- if $p \equiv 1 \pmod 4$, then $[\mathbb{Q}(P) : \mathbb{Q}] = p^2 - 1$,
- if $p \equiv 3 \pmod 4$, then $[\mathbb{Q}(P) : \mathbb{Q}] \in \{p^2 - 1, 2(p-1), (p-1)^2\}$.

Therefore, if p is an odd prime, then $[\mathbb{Q}(P) : \mathbb{Q}]$ is even.

To finish the proof, let P be a point of order a power of 2 not defined over $\mathbb{Q}$. Thanks to [6, Theorem 4.6] we see that $[\mathbb{Q}(P) : \mathbb{Q}(2P)]$ divides 2. In particular, this proves that $[\mathbb{Q}(P) : \mathbb{Q}]$ is even, since the points of order 2 on E are defined over $\mathbb{Q}$ or over a quadratic number field. ■

5. A procedure inspired by Mordell's approach. In this section, given a number field K, we provide a procedure that determines the set $S_2^0(F_4,K)$ once the sets $E_1(K)$ and $E_2(K)$ are known.

Let $L=K(\sqrt{d})$ be a quadratic extension of K, where $d\in K$ with $d\notin K^2$. Since $x\neq 0$, $y^2\neq \pm 1$, and $x^4+y^4=1$, we have $(1+y^2)/x^2=x^2/(1-y^2)$. Let

$$t=\frac{1+y^2}{x^2}\ \left(=\frac{x^2}{1-y^2}\right). \tag{5.1}$$

It is a straightforward computation to check that $t\notin\{0,\pm 1,\pm\zeta_8^2\}$. It directly follows from $x^4+y^4=1$ and (5.1) that

$$x^2=\frac{2t}{t^2+1},\qquad y^2=\frac{t^2-1}{t^2+1}. \tag{5.2}$$

Let $s=2t$, $2u=x(s^2+4)$, and $2v=xy(s^2+4)$. We deduce from (5.2) that

$$E_1\,:\,u^2=s^3+4s,\qquad E_2\,:\,v^2=s^3-4s. \tag{5.3}$$

We are going to split our procedure into two parts depending on whether $t\in K$.

Step I: $t\in K$. Let $u=a_1+b_1\sqrt{d}$ and $v=a_2+b_2\sqrt{d}$, where $a_1,a_2,b_1,b_2\in K$. From (5.3), $u^2,v^2\in K$. Since $\sqrt{d}\notin K$, $a_1b_1=a_2b_2=0$. We consider the following cases:

- $b_1=0$. Then $u=a_1\in K$. Thus $(s,u)\in E_1(K)$.
- $b_2=0$. Then $v=a_2\in K$. Thus $(s,v)\in E_2(K)$.
- $b_1b_2\neq 0$. Then $a_1=a_2=0$. It follows from (5.3) that

  $$db_1^2=s(s^2+4),\qquad db_2^2=s(s^2-4).$$

  Hence,

  $$H_3\,:\,r^2=(s^2+4)(s^2-4),$$

  where $r=db_1b_2v/s\in K$. Thus $(s,r)\in H_3(K)$. Note that the curve H_3 is $\mathbb{Q}$-isomorphic to E_1 by the map

  $$E_1\ni(x,y)\mapsto\left(\frac{2(x+2)}{x-2},\frac{16y}{(x-2)^2}\right)\in H_3.$$

In this part of the procedure, we need to compute the K-rational points of the curves E_1, E_2, and H_3. From the first coordinate of each point, we obtain s, and subsequently calculate x^2 and y^2, and finally calculate $(x,y)\in S_2^0(F_4,K)$.

Step II: $t\notin K$. Let $Q(T)\in K[T]$ be the monic minimal polynomial of s over K. Since $[L:K]=2$ and $t\notin K$, we have $\deg Q(T)=2$ and $L=K(s)$. By (5.3), there exist $\alpha_1,\alpha_2,\beta_1,\beta_2\in K$ such that

$$s^3+4s=(\alpha_1+\beta_1 s)^2,\qquad s^3-4s=(\alpha_2+\beta_2 s)^2.$$

Thus, there exist $r_1, r_2 \in K$ such that

$$T^3 + 4T - (\alpha_1 + \beta_1 T)^2 = Q(T)(T - r_1),$$
$$T^3 - 4T - (\alpha_2 + \beta_2 T)^2 = Q(T)(T - r_2).$$

Hence, $(r_j, \alpha_j + \beta_j r_j) \in E_j(K)$ for $j = 1, 2$. For $P_j = (x_j, y_j) \in E_j(K)$, let $Q_{\beta_j}(T) \in K[T]$, $j = 1, 2$, be such that

$$T^3 + 4T - (y_1 - \beta_1 x_1 + \beta_1 T)^2 = Q_{\beta_1}(T)(T - x_1),$$
$$T^3 - 4T - (y_2 - \beta_2 x_2 + \beta_2 T)^2 = Q_{\beta_2}(T)(T - x_2).$$

Note that for $j = 1, 2$, replacing P_j by $-P_j$ is equivalent to changing β_j to $-\beta_j$. Therefore, we only need to implement the computations with one element in each set $\{\pm P_j\}$.

Finally, we find $\beta_1, \beta_2 \in K$ by solving the system of quadratic equations coming from the equality $Q_{\beta_1}(T) = Q_{\beta_2}(T)$, and then we find $Q(T)$, the minimal polynomial of $s = t/2$ over K. That is, we obtain s, and subsequently calculate x^2 and y^2, and finally $(x, y) \in S_2^0(F_4, K)$.

6. Proof of Theorem 1.1

Proof of Theorem 1.1(i). In Section 5, given a number field K, we provided a procedure that allows the computation of $\Gamma_2(F_4, K)$ from the points of $E_1(K)$ and $E_2(K)$. In the particular case where $\operatorname{rank}_{\mathbb{Z}} E_j(K) = 0$, $j = 1, 2$, these sets are finite, and thus $\Gamma_2(F_4, K)$ is also finite. This proves the first part of Theorem 1.1.

A different proof comes from Theorem 2.1 along with the decomposition of the Jacobian of F_4 established in Lemma 3.1.

Proof of Theorem 1.1(ii). Notice that $j(E_1) = j(E_2) = 1728$, therefore if K is a number field of odd degree, Proposition 4.1 asserts that $E_j(K)_{\text{tors}} = E_j(\mathbb{Q})_{\text{tors}}$, $j = 1, 2$. Moreover, when $\operatorname{rank}_{\mathbb{Z}} E_j(K) = 0$ we have $E_j(K) = E_j(\mathbb{Q})$, $j = 1, 2$. Theorem 1.1(ii) follows from the procedure described in Section 5. That is, $\Gamma_2(F_4, K) = \Gamma_2(F_4, \mathbb{Q})$.

Proof of Theorem 1.1(iii). Let K be a number field such that $E_j(K)$ is finite, $j = 1, 2$. Then the procedure given in Section 5 allows the computation of $\Gamma_2(F_4, K)$ from the points of $E_1(K)_{\text{tors}}$ and $E_2(K)_{\text{tors}}$. In particular, if L is the maximal subfield contained in K such that $E_j(K)_{\text{tors}} = E_j(L)_{\text{tors}}$ for $j = 1, 2$, then $\Gamma_2(F_4, K) = \Gamma_2(F_4, L)$. This restricts the study to number fields in which the torsion grows in E_1 and/or E_2. In the Appendix, it is shown that such fields are $\mathbb{Q}(\sqrt{-1})$, $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\zeta_8)$ and $\mathbb{Q}(\alpha)$, where α satisfies $\alpha^4 - 2\alpha^2 - 1 = 0$. Note that for those fields the ranks of the elliptic curves E_1 and E_2 are 0. Therefore, it suffices to compute $\Gamma_2(F_4, K)$ for those fields, and to find $\Gamma_2(F_4, \mathbb{Q})$. For this purpose, for each of those number fields K, the required data for these points are provided in the Appendix.

STEP I. We find the affine points of $E_1(K)$, $E_2(K)$, and $H_3(K)$.

STEP II. We give a table where for each pair of points (P_1, P_2) with $P_1 \in E_1(K)$ and $P_2 \in E_2(K)$, we put ✗ if there are no solutions (β_1, β_2) in K or the corresponding quadratic polynomial $Q(x)$ is reducible or $t \in \{0, \pm 1, \pm\sqrt{-1}\}$. Otherwise, we give the corresponding irreducible quadratic minimal polynomial $Q(x)$ of s and the point in $S_2^0(F_4, K)$.

6.1. $\Gamma_2(F_4, \mathbb{Q})$**.** Then $K = \mathbb{Q}$ and

$$\begin{aligned} E_1(\mathbb{Q}) &= \{(0,0), (2, \pm 4), [0:1:0]\}, \\ E_2(\mathbb{Q}) &= \{(0,0), (\pm 2, 0), [0:1:0]\}, \\ H_3(\mathbb{Q}) &= \{(\pm 2, 0), [1:\pm 1:0]\}. \end{aligned}$$

STEP I. For each s we obtain the following points in $\Gamma_2(F_4, \mathbb{Q})$, where $m_{b/K}(T)$ denotes the minimal polynomial of the corresponding b over a number field K:

s	$(x,y) \in \Gamma_2(F_4, \mathbb{Q})$	$m_{b/\mathbb{Q}}(T)$
0	$(0, b)$	$T^2 + 1$
2	$(1, 0)$	$T - 1$
-2	$(b, 0)$	$T^2 + 1$

Note that those points in $\Gamma_2(F_4, \mathbb{Q})$ are trivial points.

STEP II. We determine the following table:

P_1 P_2	$(0,0)$	$(2,4)$
$(0,0)$	✗	✗
$(2,0)$	✗	$(-s-1, -s)$ $x^2 + x + 2$
$(-2,0)$	✗	✗

Hence, $S_2^0(F_4, \mathbb{Q}) = \{(\omega, \overline{\omega})\}$, where $\omega = (1 + \sqrt{-7})/2$ and $\overline{\omega} = (1 - \sqrt{-7})/2$. This finishes the computation of $\Gamma_2(F_4, K)$. In particular, we have shown that if F_4 has non-trivial points in a quadratic number field $\mathbb{Q}(\sqrt{d})$, then $d = -7$, which is Aigner's result [2].

6.2. $\Gamma_2(F_4, \mathbb{Q}(\sqrt{-1}))$**.** Then $K = \mathbb{Q}(\sqrt{-1})$ and

$$\begin{aligned} E_1(\mathbb{Q}(\sqrt{-1})) &= E_1(\mathbb{Q}) \cup \{(-2, \pm 4\sqrt{-1}), (\pm 2\sqrt{-1}, 0)\}, \\ E_2(\mathbb{Q}(\sqrt{-1})) &= E_2(\mathbb{Q}), \\ H_3(\mathbb{Q}(\sqrt{-1})) &= H_3(\mathbb{Q}) \cup \{(0, \pm 4\sqrt{-1}), (\pm 2\sqrt{-1}, 0)\}. \end{aligned}$$

Step I. For $s \notin \mathbb{Q}$ we compute the following points in $\mathit{\Gamma}_2(F_4, \mathbb{Q}(\sqrt{-1}))$:

s	$(x,y) \in \mathit{\Gamma}_2(F_4, \mathbb{Q}(\sqrt{-1}))$	$m_{b/\mathbb{Q}}(T)$
$2\sqrt{-1}$	$(-b, 1)$	$T^2 + \sqrt{-1}$
$-2\sqrt{-1}$	$(-b, 1)$	$T^2 - \sqrt{-1}$

Note that those points in $\mathit{\Gamma}_2(F_4, \mathbb{Q}(\sqrt{-1}))$ are trivial points.

Step II. We calculate the following tables:

P_1 P_2	$(2,4)$	$(-2, 4\sqrt{-1})$
$(0,0)$	✗	✗
$(2,0)$	$(-s-1, -s)$ $x^2 + x + 2$	$(-\frac{1}{2}\sqrt{-1}s, -\frac{1}{2}\sqrt{-1}s + \sqrt{-1})$ $x^2 - 2x + 8$
$(-2,0)$	$(-\frac{1}{2}s, -\frac{1}{2}\sqrt{-1}s - \sqrt{-1})$ $x^2 + 2x + 8$	$(-\sqrt{-1}s + \sqrt{-1}, -s)$ $x^2 - x + 2$

P_1 P_2	$(0,0)$	$(2\sqrt{-1}, 0)$	$(-2\sqrt{-1}, 0)$
$(0,0)$	✗	✗	✗
$(2,0)$	✗	✗	✗
$(-2,0)$	✗	✗	✗

Therefore, $S_2^0(F_4, \mathbb{Q}(\sqrt{-1})) = \{\sqrt{-1}(\omega, \overline{\omega}), (\sqrt{-1}\omega, \overline{\omega}), (\omega, \sqrt{-1}\overline{\omega})\}$. This finishes the computation of $\mathit{\Gamma}_2(F_4, \mathbb{Q}(\sqrt{-1}))$.

6.3. $\mathit{\Gamma}_2(F_4, \mathbb{Q}(\sqrt{2}))$. Then $K = \mathbb{Q}(\sqrt{2})$ and

$$\begin{aligned}
&E_1(\mathbb{Q}(\sqrt{2})) = E_1(\mathbb{Q}),\\
&E_2(\mathbb{Q}(\sqrt{2})) = E_2(\mathbb{Q})\\
&\qquad\qquad \cup \{\pm(2(\sqrt{2}+1), 4(\sqrt{2}+1)), \pm(2(-\sqrt{2}+1), 4(\sqrt{2}-1))\},\\
&H_3(\mathbb{Q}(\sqrt{2})) = H_3(\mathbb{Q}).
\end{aligned}$$

Step I. For $s \notin \mathbb{Q}$, we obtain the following points in $\mathit{\Gamma}_2(F_4, \mathbb{Q}(\sqrt{2}))$:

s	$(x,y) \in \mathit{\Gamma}_2(F_4, \mathbb{Q}(\sqrt{2}))$	$m_{b/\mathbb{Q}}(T)$
$2\sqrt{2} + 2$	$(-b, -b)$	$T^2 - \frac{1}{2}\sqrt{2}$
$-2\sqrt{2} + 2$	$(-b, -b)$	$T^2 + \frac{1}{2}\sqrt{2}$

We obtain the following points in $S_2^0(F_4, \mathbb{Q}(\sqrt{2}))$:

$$(1/\sqrt[4]{2}, 1/\sqrt[4]{2}), \quad \sqrt{-1}(1/\sqrt[4]{2}, 1/\sqrt[4]{2}).$$

STEP II. We compute the following table:

P_1 P_2	$(0,0)$	$(2,4)$
$(0,0)$	✗	✗
$(2,0)$	✗	$(-s-1,-s)$ x^2+x+2
$(-2,0)$	✗	✗
$(2(\sqrt{2}+1), 4(\sqrt{2}+1))$	✗	✗
$(2(-\sqrt{2}+1), 4(-\sqrt{2}+1))$	✗	✗

Therefore, $S_2^0(F_4, \mathbb{Q}(\sqrt{2})) = \{(1/\sqrt[4]{2}, 1/\sqrt[4]{2}), \sqrt{-1}(1/\sqrt[4]{2}, 1/\sqrt[4]{2})\}$. This finishes the proof for the computation of $S_2^0(F_4, \mathbb{Q}(\sqrt{2}))$.

6.4. $\Gamma_2(F_4, \mathbb{Q}(\alpha))$**.** Then $\sqrt{2} = 1 - \alpha^2$, $K = \mathbb{Q}(\alpha)$, and

$$\begin{aligned} E_1(\mathbb{Q}(\alpha)) &= E_1(\mathbb{Q}) \cup \{\pm S_{1,1}, \pm S_{1,2}\}, \\ E_2(\mathbb{Q}(\alpha)) &= E_2(\mathbb{Q}(\sqrt{2})), \\ H_3(\mathbb{Q}(\alpha)) &= H_3(\mathbb{Q}) \cup \{(\pm 2\alpha, \pm 4(\alpha^3 - \alpha))\}. \end{aligned}$$

STEP I. For $s \notin \mathbb{Q}(\sqrt{2})$ we determine the following points in $\Gamma_2(F_4, \mathbb{Q}(\alpha))$:

s	$(x,y) \in \Gamma_2(F_4, \mathbb{Q}(\alpha))$	$m_{b/\mathbb{Q}(\alpha)}(T)$
-2α	$(b, -\alpha^3 + 2\alpha)$	$T^2 - \alpha^3 + 3\alpha$
$-2\alpha^3 + 2\alpha^2 + 2\alpha$	$(-\alpha^3 + 2\alpha, b)$	$T^2 - \alpha^3 + 3\alpha$
2α	$(b, -\alpha^3 + 2\alpha)$	$T^2 + \alpha^3 - 3\alpha$
$2\alpha^3 + 2\alpha^2 - 2\alpha$	$(-\alpha^3 + 2\alpha, b)$	$T^2 + \alpha^3 - 3\alpha$

We obtain the points $(\delta, -\alpha^3 + 2\alpha), (\sqrt{-1}\delta, -\alpha^3 + 2\alpha)$ in $S_2^0(F_4, \mathbb{Q}(\alpha))$, where δ satisfies $\delta^2 = \alpha^3 - 3\alpha$.

STEP II. The (P_1, P_2) table appears on the next page. No new points come in the second step. Therefore,

$$S_2^0(F_4, \mathbb{Q}(\alpha)) = \{(\delta, -\alpha^3 + 2\alpha), (\sqrt{-1}\delta, -\alpha^3 + 2\alpha)\}.$$

This finishes the computation of $\Gamma_2(F_4, \mathbb{Q}(\alpha))$.

P_1 P_2	$(0,0)$	$(2,4)$	$S_{1,1}$	$S_{1,2}$
$(0,0)$	✗	✗	✗	✗
$(2,0)$	✗	$(-s-1,-s)$ x^2+x+2	✗	✗
$(-2,0)$	✗	✗	✗	✗
$(2(\sqrt{2}+1),4(\sqrt{2}+1))$	✗	✗	✗	✗
$(2(-\sqrt{2}+1),4(-\sqrt{2}+1))$	✗	✗	✗	✗

6.5. $\Gamma_2(F_4,\mathbb{Q}(\zeta_8))$**.** Then $K=\mathbb{Q}(\zeta_8)$ and

$$\begin{aligned}
&E_1(\mathbb{Q}(\zeta_8)) = E_1(\mathbb{Q}(\sqrt{-1}))\cup\{\pm R_{1,1},\pm R_{1,2},\pm R_{1,3},\pm R_{1,4}\},\\
&E_2(\mathbb{Q}(\zeta_8)) = E_2(\mathbb{Q})\cup\{\pm R_{2,1},\pm R_{2,2},\pm R_{2,3},\pm R_{2,4}\},\\
&H_3(\mathbb{Q}(\zeta_8)) = H_3(\mathbb{Q}(\sqrt{-1}))\cup(\pm 2\zeta_8^3,\pm 4(\zeta_8^3+\zeta_8)),(\pm 2\zeta_8,\pm 4(\zeta_8^3+\zeta_8))\}.
\end{aligned}$$

Step I. For $s\notin\mathbb{Q}(\sqrt{-1})=\mathbb{Q}(\zeta_8^2)$ and $s\notin\mathbb{Q}(\sqrt{2})=\mathbb{Q}(\zeta_8^3-\zeta_8)$, we deduce the following points in $\Gamma_2(F_4,\mathbb{Q}(\zeta_8))$:

s	$(x,y)\in\Gamma_2(F_4,\mathbb{Q}(\zeta_8))$	$m_{b/\mathbb{Q}(\zeta_8)}(T)$
$2\zeta_8$	$(-b,-\zeta_8)$	$T^2+\sqrt{2}$
$-2\zeta_8^3-2\zeta_8^2-2\zeta_8$	$(-\zeta_8,-b)$	$T^2+\sqrt{2}$
$-2\zeta_8^3$	$(-b,-\zeta_8^3)$	$T^2+\sqrt{2}$
$2\zeta_8^3+2\zeta_8^2+2\zeta_8$	$(-\zeta_8^3,-b)$	$T^2+\sqrt{2}$
$-2\zeta_8$	$(-b,-\zeta_8)$	$T^2-\sqrt{2}$
$2\zeta_8^3-2\zeta_8^2+2\zeta_8$	$(-\zeta_8,-b)$	$T^2-\sqrt{2}$
$2\zeta_8^3$	$(-b,-\zeta_8^3)$	$T^2-\sqrt{2}$
$-2\zeta_8^3+2\zeta_8^2-2\zeta_8$	$(-\zeta_8^3,-b)$	$T^2-\sqrt{2}$
$2\zeta_8^3-2\zeta_8-2$	$(-b,-\zeta_8^2 b)$	$T^2+\frac{1}{2}(-\zeta_8^3+\zeta_8)$
$-2\zeta_8^3+2\zeta_8-2$	$(-b,-\zeta_8^2 b)$	$T^2+\frac{1}{2}(\zeta_8^3-\zeta_8)$

We obtain the following points in $S_2^0(F_4,\mathbb{Q}(\zeta_8))$:

$$(\zeta_8,\sqrt[4]{2}),\quad(\zeta_8^3,\sqrt[4]{2}),\quad(\zeta_8,\zeta_8^2\sqrt[4]{2}),\quad(\zeta_8^3,\zeta_8^2\sqrt[4]{2})\},\quad(1/\sqrt[4]{2},\zeta_8^2/\sqrt[4]{2}).$$

Step II. In the following table, for each pair of points $P_j\in E_j(\mathbb{Q}(\zeta_8))$, $j=1,2$, such that the corresponding position in Table 1 below is not a ✗ and it is primitive in $\mathbb{Q}(\zeta_8)$, we simplify the corresponding point in $S_2^0(F_4,\mathbb{Q}(\zeta_8))$:

$(\frac{1}{4}(-\zeta_8^3+\zeta_8)s+\frac{1}{2}(-\zeta_8^3+\zeta_8), \frac{1}{4}(-\zeta_8^3+\zeta_8)s+\frac{1}{2}(\zeta_8^3+\zeta_8))$ $s^2+(2+2\zeta_8^2)s-4\zeta_8^2=0$	$(\zeta_3\zeta_8^3, -\zeta_3^2\zeta_8^3)$
$(\frac{1}{4}(-\zeta_8^3+\zeta_8)s+\frac{1}{2}(-\zeta_8^3+\zeta_8), \frac{1}{4}(-\zeta_8^3+\zeta_8)s+\frac{1}{2}(-\zeta_8^3-\zeta_8))$ $s^2+(-2\zeta_8^2+2)s+4\zeta_8^2=0$	$(-\zeta_3^2\zeta_8, \zeta_3\zeta_8)$
$(\frac{1}{4}(-\zeta_8^3-\zeta_8)s+\frac{1}{2}(\zeta_8^3+\zeta_8), \frac{1}{4}(-\zeta_8^3+\zeta_8)s+\frac{1}{2}(\zeta_8^3+\zeta_8))$ $s^2+(2\zeta_8^2-2)s+4\zeta_8^2=0$	$(-\zeta_3\zeta_8^3, -\zeta_3^2\zeta_8)$
$(\frac{1}{4}(-\zeta_8^3-\zeta_8)s+\frac{1}{2}(\zeta_8^3+\zeta_8), \frac{1}{4}(-\zeta_8^3+\zeta_8)s+\frac{1}{2}(-\zeta_8^3-\zeta_8))$ $s^2+(-2\zeta_8^2-2)s-4\zeta_8^2=0$	$(-\zeta_3^2\zeta_8, \zeta_3\zeta_8^3)$
$(\frac{1}{8}(-\zeta_8^2+1)s+\frac{1}{4}(-\zeta_8^2-3), \frac{1}{8}(-\zeta_8^3-\zeta_8)s+\frac{1}{4}(3\zeta_8^3+3\zeta_8))$ $s^2+(-6\zeta_8^2-6)s+4\zeta_8^2=0$	$\omega^{-1}(-\zeta_8^2, -\varpi\zeta_8)$
$(\frac{1}{8}(-\zeta_8^2+1)s+\frac{1}{4}(-3\zeta_8^2-1), \frac{1}{8}(-\zeta_8^3-\zeta_8)s+\frac{1}{4}(-3\zeta_8^3-3\zeta_8))$ $s^2+(-6\zeta_8^2+6)s-4\zeta_8^2=0$	$\varpi^{-1}(-1, \omega\zeta_8^3)$
$(-\frac{1}{2}\zeta_8 s+\frac{1}{2}\zeta_8^3, -\frac{1}{2}\zeta_8^2 s+\frac{1}{2})$ $s^2+\zeta_8^2 s-2=0$	$\omega^{-1}(-\varpi\zeta_8^3, 1)$
$(-\frac{1}{4}\zeta_8^3 s+\zeta_8, -\frac{1}{4}s)$ $s^2+2\zeta_8^2 s-8=0$	$\varpi^{-1}(-\omega\zeta_8, \zeta_8^2)$
$(\frac{1}{8}(-\zeta_8^2-1)s+\frac{1}{4}(-\zeta_8^2+3), \frac{1}{8}(-\zeta_8^3-\zeta_8)s+\frac{1}{4}(3\zeta_8^3+3\zeta_8))$ $s^2+(6\zeta_8^2-6)s-4\zeta_8^2=0$	$\varpi^{-1}(-\zeta_8^2, -\omega\zeta_8^3)$
$(\frac{1}{8}(-\zeta_8^2-1)s+\frac{1}{4}(-3\zeta_8^2+1), \frac{1}{8}(-\zeta_8^3-\zeta_8)s+\frac{1}{4}(-3\zeta_8^3-3\zeta_8))$ $s^2+(6\zeta_8^2+6)s+4\zeta_8^2=0$	$\omega^{-1}(1, \varpi\zeta_8)$
$(-\frac{1}{4}\zeta_8 s+\zeta_8^3, -\frac{1}{4}s)$ $s^2-2\zeta_8^2 s-8=0$	$\omega^{-1}(-\varpi\zeta_8^3, -\zeta_8^2)$
$(-\frac{1}{2}\zeta_8^3 s+\frac{1}{2}\zeta_8, -\frac{1}{2}\zeta_8^2 s-\frac{1}{2})$ $s^2-\zeta_8^2 s-2=0$	$\omega^{-1}(-\varpi\zeta_8, -1)$

We obtain the following points in $S_2^0(F_4, \mathbb{Q}(\zeta_8))$:

$$\begin{gathered}(\zeta_3\zeta_8, \zeta_3^2\zeta_8), \quad (\zeta_3\zeta_8^3, \zeta_3^2\zeta_8^3), \quad (\zeta_3\zeta_8, \zeta_3^2\zeta_8^3), \quad (\zeta_3\zeta_8^3, \zeta_3^2\zeta_8),\\ \omega^{-1}(\varpi\zeta_8, 1), \quad \omega^{-1}(\varpi\zeta_8^3, 1), \quad \omega^{-1}(\varpi\zeta_8, \zeta_8^2), \quad \omega^{-1}(\varpi\zeta_8^3, \zeta_8^2),\\ \varpi^{-1}(\omega\zeta_8, 1), \quad \varpi^{-1}(\omega\zeta_8^3, 1), \quad \varpi^{-1}(\omega\zeta_8, \zeta_8^2), \quad \varpi^{-1}(\omega\zeta_8^3, \zeta_8^2).\end{gathered}$$

This finishes the computation of $S_2^0(F_4, \mathbb{Q}(\zeta_8))$ and in particular of the set $\Gamma_2(F_4, \mathbb{Q}(\zeta_8))$.

Proof of Theorem 1.1(iv). It is a straightforward consequence of the method described in Section 5 for computing $\Gamma_2(F_4, K)$ via the sets $E_i(K) = E_i(L)$ for $i = 1, 2$.

Table 1. Part 1

P_1 P_2	$(2,4)$	$(-2,4\sqrt{-1})$
$(0,0)$	✗	✗
$(2,0)$	$(-s-1,-s)$ x^2+x+2	$(-\frac{1}{2}\zeta_8^2 s,-\frac{1}{2}\zeta_8^2 s+\zeta_8^2)$ x^2-2x+8
$(-2,0)$	$(-\frac{1}{2}\zeta_8,-\frac{1}{2}\zeta_8^2 s-\zeta_8^2)$ x^2+2x+8	$(-\zeta_8^2 s+\zeta_8^2,-s)$ x^2-x+2
$R_{2,1}$	$(\frac{1}{8}(-\zeta_8^2+1)s+\frac{1}{4}(-\zeta_8^2-3),$ $\frac{1}{8}(-\zeta_8^3-\zeta_8)s+\frac{1}{4}(3\zeta_8^3+3\zeta_8))$ $x^2+(-6\zeta_8^2-6)x+4\zeta_8^2$	$(\frac{1}{8}(-\zeta_8^2+1)s+\frac{1}{4}(-3\zeta_8^2-1),$ $\frac{1}{8}(-\zeta_8^3-\zeta_8)s+\frac{1}{4}(-3\zeta_8^3-3\zeta_8))$ $x^2+(-6\zeta_8^2+6)x-4\zeta_8^2$
$R_{2,2}$	$(\frac{1}{8}(-\zeta_8^2-1)s+\frac{1}{4}(-\zeta_8^2+3),$ $\frac{1}{8}(-\zeta_8^3-\zeta_8)s+\frac{1}{4}(3\zeta_8^3+3\zeta_8))$ $x^2+(6\zeta_8^2-6)x-4\zeta_8^2$	$(\frac{1}{8}(-\zeta_8^2-1)s+\frac{1}{4}(-3\zeta_8^2+1),$ $\frac{1}{8}(-\zeta_8^3-\zeta_8)s+\frac{1}{4}(-3\zeta_8^3-3\zeta_8))$ $x^2+(6\zeta_8^2+6)x+4\zeta_8^2$
$R_{2,3}$	✗	✗
$R_{2,4}$	✗	✗
$R_{2,5}$	✗	✗
$R_{2,6}$	✗	✗

Table 1. Part 2

P_1 P_2	$(2\sqrt{-1},0)$	$(-2\sqrt{-1},0)$
$(0,0)$	✗	✗
$(2,0)$	$(\frac{1}{4}(-\zeta_8^3+\zeta_8)s+\frac{1}{2}(-\zeta_8^3+\zeta_8),$ $\frac{1}{4}(-\zeta_8^3+\zeta_8)s+\frac{1}{2}(\zeta_8^3+\zeta_8))$ $x^2+(2+2\zeta_8^2)x-4\zeta_8^2=0$	$(\frac{1}{4}(-\zeta_8^3+\zeta_8)s+\frac{1}{2}(-\zeta_8^3+\zeta_8),$ $\frac{1}{4}(-\zeta_8^3+\zeta_8)s+\frac{1}{2}(-\zeta_8^3-\zeta_8))$ $x^2+(-2\zeta_8^2+2)x+4\zeta_8^2=0$
$(-2,0)$	$(\frac{1}{4}(-\zeta_8^3-\zeta_8)s+\frac{1}{2}(\zeta_8^3+\zeta_8),$ $\frac{1}{4}(-\zeta_8^3+\zeta_8)s+\frac{1}{2}(\zeta_8^3+\zeta_8))$ $x^2+(2\zeta_8^2-2)x+4\zeta_8^2=0$	$(\frac{1}{4}(-\zeta_8^3-\zeta_8)s+\frac{1}{2}(\zeta_8^3+\zeta_8),$ $\frac{1}{4}(-\zeta_8^3+\zeta_8)s+\frac{1}{2}(-\zeta_8^3-\zeta_8))$ $x^2+(-2\zeta_8^2-2)x-4\zeta_8^2=0$
$R_{2,1}$	$(-\frac{1}{2}\zeta_8 s+\frac{1}{2}\zeta_8^3,-\frac{1}{2}\zeta_8^2 s+\frac{1}{2})$ $x^2+\zeta_8^2 x-2=0$	$(-\frac{1}{4}\zeta_8^3 s+\zeta_8,-\frac{1}{4}s)$ $x^2+2\zeta_8^2 x-8=0$
$R_{2,2}$	$(-\frac{1}{4}\zeta_8 s+\zeta_8^3,-\frac{1}{4}s)$ $x^2-2\zeta_8^2 x-8=0$	$(-\frac{1}{2}\zeta_8^3 s+\frac{1}{2}\zeta_8,-\frac{1}{2}\zeta_8^2 s-\frac{1}{2})$ $x^2-\zeta_8^2 x-2=0$
$R_{2,3}$	✗	✗
$R_{2,4}$	✗	✗
$R_{2,5}$	✗	✗
$R_{2,6}$	✗	✗

Table 1. Part 3

P_1 P_2	$(0,0)$	$R_{1,1}$	$R_{1,2}$	$R_{1,3}$	$R_{1,4}$
$(0,0)$	✗	✗	✗	✗	✗
$(2,0)$	✗	✗	✗	✗	✗
$(-2,0)$	✗	✗	✗	✗	✗
$R_{2,1}$	✗	✗	✗	✗	✗
$R_{2,2}$	✗	✗	✗	✗	✗
$R_{2,3}$	✗	✗	✗	✗	✗
$R_{2,4}$	✗	✗	✗	✗	✗
$R_{2,5}$	✗	✗	✗	✗	✗
$R_{2,6}$	✗	✗	✗	✗	✗

Appendix. In Section 5 a procedure was presented that, given a number field K such that $E_1(K)$ and $E_2(K)$ are finite, allows one to determine $\Gamma_2(F_4,K)$. Therefore, this reduces to determining the growth of the torsion of E_1 and E_2 over number fields. Note that E_2 is the -1-twist of E_1. In particular, they are isomorphic over $\mathbb{Q}(\zeta_8)$. Let

$$\begin{aligned}
R_{1,1} &= (2(\zeta_8^3+\zeta_8^2+\zeta_8), 4(\zeta_8^3+\zeta_8^2-1)),\\
R_{1,2} &= (2(-\zeta_8^3-\zeta_8^2-\zeta_8), 4(\zeta_8^2+\zeta_8+1)),\\
R_{1,3} &= (2(-\zeta_8^3+\zeta_8^2-\zeta_8), 4(\zeta_8^3-\zeta_8^2+1)),\\
R_{1,4} &= (2(\zeta_8^3-\zeta_8^2+\zeta_8), 4(\zeta_8^2-\zeta_8+1)),\\
S_{1,1} &= (2(\alpha^3+\alpha^2-\alpha), 4(\alpha^3+\alpha^2+1)),\\
S_{1,2} &= (2(-\alpha^3+\alpha^2+\alpha), 4(\alpha^3-\alpha^2-1)),\\
R_{2,1} &= (2\zeta_8^2, 4\zeta_8^3)),\\
R_{2,2} &= (-2\zeta_8^2, 4\zeta_8),\\
R_{2,3} &= (2(\zeta_8^3-\zeta_8-1), 4(\zeta_8^3+\zeta_8^2+\zeta_8)),\\
R_{2,4} &= (2(-\zeta_8^3+\zeta_8-1), 4(\zeta_8^3-\zeta_8^2+\zeta_8)),\\
R_{2,5} &= (2(\zeta_8^3-\zeta_8+1), 4(\zeta_8^3-\zeta_8+1)),\\
R_{2,6} &= (-2(\zeta_8^3+\zeta_8+1), 4(\zeta_8^3-\zeta_8-1)).
\end{aligned}$$

The following table illustrates the growth of the torsion of the elliptic curve E_1 in the cases where the degree is less than 8. This information has been obtained (¹) from the LMFDB database [11]; the LMFDB label for E_1 is `32.a4`. In each row, the second column displays the structure of the torsion over the number field K listed in the first column. The third

---

(¹) Torsion growth data were computed by Filip Najman and the author [7].

column shows the points in $E_1(K)_{\mathrm{tors}}$ not coming from $E_1(K')_{\mathrm{tors}}$ for any proper subfield K' of K. The diagram below shows all the number fields (of degree < 8) involved in the torsion growth of E_1. Note that α satisfies $\alpha^4 - 2\alpha^2 - 1 = 0$.

K	$E_1(K)_{\mathrm{tors}}$	Data $E_1(K)_{\mathrm{tors}}$
$\mathbb{Q}$	$\mathbb{Z}/4\mathbb{Z}$	$(0,0)$, $\pm(2,4)$
$\mathbb{Q}(\sqrt{-1})$	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$	$\pm(-2,-4\sqrt{-1}), (\pm 2\sqrt{-1}, 0)$
$\mathbb{Q}(\zeta_8)$	$\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$	$\pm R_{1,1}, \pm R_{1,2}, \pm R_{1,3}, \pm R_{1,4}$
$\mathbb{Q}(\alpha)$	$\mathbb{Z}/8\mathbb{Z}$	$\pm S_{1,1}, \pm S_{1,2}$

Similarly, for the elliptic curve E_2 (whose LMFDB label is `64.a3`) we obtain

K	$E_2(K)_{\mathrm{tors}}$	Data $E_2(K)_{\mathrm{tors}}$
$\mathbb{Q}$	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$	$(0,0)$, $(\pm 2, 0)$
$\mathbb{Q}(\sqrt{2})$	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$	$\pm(2(\sqrt{2}+1), 4(\sqrt{2}+1))$ $\pm(2(-\sqrt{2}+1), 4(\sqrt{2}-1))$
$\mathbb{Q}(\zeta_8)$	$\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$	$\pm R_{2,1}, \pm R_{2,2}, \pm R_{2,3}, \pm R_{2,4}, \pm R_{2,5}, \pm R_{2,6}$

The following diagram illustrates the lattice of number fields associated with the growth of the torsion of the elliptic curves E_1 and E_2:

$$\begin{tikzcd}
& \mathbb{Q}(\zeta_8) \arrow[ld, dash] \arrow[rd, dash] & & \mathbb{Q}(\alpha) \arrow[ld, dash] \\
\mathbb{Q}(\sqrt{-1}) \arrow[rd, dash] & & \mathbb{Q}(\sqrt{2}) \arrow[ld, dash] & \\
& \mathbb{Q} & &
\end{tikzcd}$$

Some computations. In this section, we show some number fields that fulfill the conditions required for the application of Theorem 1.1.

The following list shows all the square-free integers $D \neq -1, 2$, $|D| < 200$, satisfying the condition $\operatorname{rank}_{\mathbb{Z}} E_1(\mathbb{Q}(\sqrt{D})) = \operatorname{rank}_{\mathbb{Z}} E_2(\mathbb{Q}(\sqrt{D}) = 0$:

$$-2,\ \pm 33,\ \pm 57,\ \pm 66,\ \pm 73,\ \pm 89,\ \pm 114,\ \pm 129,\ \pm 146,\ \pm 177,\ \pm 178,\ \pm 185.$$

In the following table we show the defining polynomials of five number fields K such that

$$\operatorname{rank}_{\mathbb{Z}} E_1(K) = \operatorname{rank}_{\mathbb{Z}} E_2(K) = 0 \quad \text{for } [K:\mathbb{Q}] = d \text{ with } d = 3, 4, 5.$$

$[K:\mathbb{Q}]=3$	$[K:\mathbb{Q}]=4$	$[K:\mathbb{Q}]=5$
x^3-x^2-2x+1	x^4+1	$x^5+x^3-2x^2-1$
x^3-3x-1	x^4+x^2-x+1	$x^5-x^4+x^3-x^2+2x-1$
x^3-x^2-4x-1	x^4+x^2-2x+1	x^5-x^3+2x-1
x^3-x^2+2x+2	x^4-2x^3+2	$x^5-x^4+x^3-x^2+1$
x^3-x^2-4x+1	$x^4-2x^3+x^2-2x+1$	$x^5-x^4+x^3+x-1$

For the degree 6 or 7 cases, we were only able to identify the number field $\mathbb{Q}(\delta)$ with δ having minimal polynomial $x^6-x^4-2x^3+2x+1$ that fulfill the conditions required for the application of Theorem 1.1. In most number fields where we attempted to demonstrate that $\operatorname{rank}_{\mathbb{Z}} E_j(K)=0$, $j=1,2$, `Magma` was unable to perform the computation. Consequently, we opted to compute the analytic rank, but this also proved unsuccessful. Our final approach was to determine whether $L(E_1/K,1)$ and $L(E_2/K,1)$ vanish or not. However, this method also failed to provide new number fields satisfying the conditions required to apply Theorem 1.1.

Funding. This research was partly supported by the grant PID2022-138916NB-I00 funded by MCIN/AEI/10.13039/501100011033 and by ERDF "A way of making Europe".

References

[1] D. Abramovich and J. Harris, *Abelian varieties and curves in $W_d(C)$*, Compos. Math. 78 (1991), 227–238.

[2] A. Aigner, *Über die Möglichkeit von $x^4+y^4=z^4$ in quadratischen Körpern*, Jahresber. Deutsch. Math.-Verein. 43 (1934), 226–229.

[3] F. Bars, *On quadratic points of classical modular curves*, in: Number Theory Related to Modular Curves: Momose Memorial Volume, Contemp. Math. 701, Amer. Math. Soc., Providence, RI, 2018, 17–34.

[4] W. Bosma, J. Cannon, and C. Playoust, *The `Magma` algebra system I: the user language*, J. Symbolic Comput. 24 (1997), 235–265.

[5] E. González-Jiménez, *Quadratic points on the Fermat quartic over number fields, `Magma` source*, https://matematicas.uam.es/∼enrique.gonzalez.jimenez/.

[6] E. González-Jiménez and F. Najman, *Growth of torsion groups of elliptic curves upon base change*, Math. Comp. 89 (2020), 1457–1485.

[7] E. González-Jiménez and F. Najman, *An algorithm for determining torsion growth of elliptic curves*, Experiment. Math. 32 (2023), 70–81.

[8] J. Harris and J. H. Silverman, *Bielliptic curves and symmetric products*, Proc. Amer. Math. Soc. 112 (1991), 347–356.

[9] Y. Ishitsuka, T. Ito, and T. Ohshita, *Explicit calculation of the mod 4 Galois representation associated with the Fermat quartic*, Int. J. Number Theory 16 (2020), 881–905.

[10] M. Khawaja and F. Jarvis, *Fermat's last theorem over* $\mathbb{Q}(\sqrt{2},\sqrt{3})$, Algebra Number Theory 19 (2025), 457–480.

[11] The LMFDB Collaboration, *The L-functions and modular forms database*, https://www.lmfdb.org, 2024, accessed 15 July 2024.

[12] L. J. Mordell, *The Diophantine equation* $x^4+y^4=1$ *in algebraic number fields*, Acta Arith. 14 (1968), 347–355.

[13] E. Ozman and S. Siksek, *Quadratic points on modular curves*, Math. Comp. 88 (2019), 2461–2484.

[14] J. H. Silverman, *The Arithmetic of Elliptic Curves*, 2nd ed., Grad. Texts in Math. 106, Springer, Dordrecht, 2009.

[15] J. H. Silverman, *Advanced Topics in the Arithmetic of Elliptic Curves*, Grad. Texts in Math. 151, Springer, New York, 1994.

[16] N. X. Tho, *Points on* $x^4+y^4=z^4$ *over quadratic extensions of* $\mathbb{Q}(\zeta_8)(T_1,T_2,\dots,T_n)$, Bull. Austral. Math. Soc. 111 (2025), 19–31.

[17] D. J. Zywina, *On the possible images of the mod* ℓ *representations associated to elliptic curves over* $\mathbb{Q}$, arXiv:1508.07660v1 (2015).

Enrique González-Jiménez
Departamento de Matemáticas
Universidad Autónoma de Madrid
Madrid, Spain
E-mail: enrique.gonzalez.jimenez@uam.es