数域上的费马四次曲线的二次点

ENRIQUE GONZALEZ–JIMENEZ

Abstract. 设 C 是定义在数域 K上的一条曲线。若点 $P \in C(\mathbb{Q})$满足 $[K(P): K] = 2$, 则称其为 K二次点。设 K 是一个数域，椭圆曲线$E_1: y^2 = x^3 + 4x$ 和 $E_2: y^2 = x^3 - 4x$ 在 K 上的秩均为 0。在上述条件下，我们证明费马四次曲线 $F_4: X^4 + Y^4 = Z^4$ 上的 K二次点集有限且可计算，并给出计算该有限集合的步骤。特别地，当 $[K: \mathbb{Q}] < 8$时，我们显式计算出所有K二次点。此外，若 K 的次数为奇数，我们证明所有K二次点恰好对应于 $\mathbb{Q}$二次点。

arXiv:2602.01398v1 [math.NT] 1 Feb 2026

1. Introduction

费马于 1637 年证明，费马四次曲线 $F_4: X^4 + Y^4 = Z^4$ 只有平凡解（即$XY = 0$）。此后，众多数学家研究了该方程在数域上的解。设 K 为一个数域，并用 $F_4(K)$ 表示 F_4的 K-有理点集。本文旨在确定 F_4上的 K-二次点集:

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

Aigner [2] 给出了 $\Gamma_2(F_4, \mathbb{Q})$，并证明 $\mathbb{Q}(\sqrt{-7})$ 是包含非平凡解的唯一二次扩张（注意，$(1 + \sqrt{-7})^4 + (1 - \sqrt{-7})^4 = 2^4$）。Ishitsuka 等人 [9, 定理 7.3]给出了 $\Gamma_2(F_4, \mathbb{Q}(\zeta_8))$，其中 ζ_8 是一个本原 8^{th}次单位根。最近，Tho [16], 运用 Mordell 的方法 [11], 给出了不同于 Ishitsuka 等人所给证明的另一种证明。完成这项工作后，我们得知 Khawaja 和 Jarvis [10, 第 3 节、定理 6.4] 此前已研究过确定落在$\mathbb{Q}(\sqrt{2})$的二次扩张中的费马四次曲线上的点这一问题。具体而言，他们证明所有此类点都落在以下域之一: $\mathbb{Q}(\sqrt{2}, \sqrt{-1})$,$\mathbb{Q}(\sqrt{2}, \sqrt{-7})$, $\mathbb{Q}(\sqrt[4]{2})$, 或 $\mathbb{Q}(\sqrt{-1}\sqrt[4]{2})$。我们注意到，他们使用的方法本质上与 Tho [16], 所用的方法相同，而后者构成了本文的基础。与以往的文章不同，本文利用椭圆曲线 $E_1: y^2 = x^3 + 4x$和 $E_2: y^2 = x^3 - 4x$ 的挠点增长知识，来推广先前的结果。

在本文中，我们使用 Mordell 方法给出一种在集合有限的情形下计算 $\Gamma_2(F_4, K)$ 的步骤。特别地，若 K 的次数为奇数且 $\Gamma_2(F_4, K)$ 为有限集，我们证明 $\Gamma_2(F_4, K) = \Gamma_2(F_4, \mathbb{Q})$。最后，若 $[K: \mathbb{Q}] < 8$，我们显式计算有限集 $\Gamma_2(F_4, K)$。

注意，若 $\overline{\mathbb{Q}}$表示 $\mathbb{Q}$ 的代数闭包，则 $F_4(\mathbb{Q})$ 具有如下平凡点:

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

特别地，$[0: \pm 1: 1], [0: \pm\zeta_8^2: 1], [\pm 1: 0: 1], [\pm\zeta_8^2: 0: 1] \in \Gamma_2(F_4, \mathbb{Q})$，以及 $[1: \zeta_8^j: 0] \in \Gamma_2(F_4, K)$，对 $j = 1, 3, 5, 7$ 成立，当且仅当 $\mathbb{Q}(\sqrt{2}) \subset K$ 或 $\mathbb{Q}(\sqrt{-1}) \subset K$。

设 $Z \neq 0$。变量替换 $x = X/Z$ 和 $y = Y/Z$ 给出仿射方程

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

Date: 2026年2月3日。2020 *Mathematics Subject Classification.* 主分类号 11D25、14G05；次分类号 14H52、11G05。*Key words and phrases.* 椭圆曲线、费马四次曲线、二次点。作者获得西班牙科学与创新部/西班牙国家研究署/10.13039/501100011033资助的 PID2022-138916NB-I00资助项目，并获欧洲区域发展基金资助。欧洲区域发展基金: 建设欧洲之路。

注意，若 K 是一个数域，且 $(x,y)\in F_4^0(K)$，那么 $(\pm x,\pm y)$、$(\pm y,\pm x)\in F_4^0(K)$。若对于任意真子域 $K'\subset K$，都有 $(x,y)\notin F_4^0(K')$，则称 $(x,y)\in F_4^0(K)$ 是 F_4^0（或 F_4）的本原点。令 $S_2^0(F_4,K)$ 表示从 $\Gamma_2(F_4,K)$ 中移除所有平凡点和非本原点，并且对于每个集合 $\{(\pm x,\pm y)、(\pm y,\pm x)\}$仅保留一个代表元 (x,y) 后得到的集合。

设椭圆曲线为 $E_1:\ y^2=x^3+4x$ 与 $E_2:\ y^2=x^3-4x$。本文的主要结果如下：

定理 1. 设 K 为一个数域，使得秩$_{\mathbb{Z}}E_j(K)=0,\ j=1,2$。则：

(i) $\Gamma_2(F_4,K)$ 是有限且可计算的。*(ii)* 若 $[K:\mathbb{Q}]$ 为奇数，则 $\Gamma_2(F_4,K)=\Gamma_2(F_4,\mathbb{Q})$。*(iii)* 若 $[K:\mathbb{Q}]<8$，则 $\Gamma_2(F_4,K)=\Gamma_2(F_4,L)$，其中 $L\in\{\mathbb{Q},\mathbb{Q}(\sqrt{-1})\ \mathbb{Q}(\sqrt{2})\ \mathbb{Q}(\zeta_8)\ \mathbb{Q}(\alpha)\}$ (α 满足 $\alpha^4-2\alpha^2-1=0$) 是使得 $L\subseteq K$ 成立的最大数域。此外，集合 $S_2^0(F_4,L)$ 出现在下表中

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

$\zeta_3=e^{2i\pi/3}$, $\omega=(1+\sqrt{-7})/2$, α 满足 $\alpha^4-2\alpha^2-1=0$ 且 δ 满足 $\delta^2=\alpha^3-3\alpha$。

（*iv*）设 L 为一个数域，使得 $E_i(K)=E_i(L)$ 对 $i=1,2$ 成立。则 $\Gamma_2(F_4,K)=\Gamma_2(F_4,L)$.

以下推论是前述定理的直接结果：

推论 2。我们有

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

推论 3。设 K 为一个数域。那么，在以下情况下，F_4 在二次扩张 L/K 中具有非平凡的本原点：

(i) 若 $K=\mathbb{Q}$，则 $L=\mathbb{Q}(\sqrt{-7})$。*(ii)* 若 $K=\mathbb{Q}(\sqrt{-1})$，则 $L=\mathbb{Q}(\sqrt{-1},\sqrt{-7})$。（*iii*）若 $K=\mathbb{Q}(\sqrt{2})$，则 $L=\mathbb{Q}(\sqrt[4]{2})$ 或 $L=\mathbb{Q}(\sqrt{-1}\sqrt[4]{2})$。（*iv*）若 $K=\mathbb{Q}(\alpha)$，则 $L=\mathbb{Q}(\alpha,\sqrt{\alpha^3-3\alpha})$ 或 $L=\mathbb{Q}(\alpha,\sqrt{-\alpha^3+3\alpha})$。（*v*）若 $K=\mathbb{Q}(\zeta_8)$，则 $L=\mathbb{Q}(\zeta_8,\sqrt[4]{2})$、$L=\mathbb{Q}(\zeta_8,\sqrt{-3})$，或 $L=\mathbb{Q}(\zeta_8,\sqrt{-7})$。

特别地，(i) 是 Aigner 的结果，(v) 是 Ishitsuka 等人的结果。

备注： 定理 1 (iv) 的一个直接推论是，对于满足 $[K:\mathbb{Q}]>8$ 的某些数域 K，可以计算 $\Gamma_2(F_4,K)$。例如，当 $K=\mathbb{Q}(\zeta_{16})$ 时，我们有 $\Gamma_2(F_4,\mathbb{Q}(\zeta_{16}))=\Gamma_2(F_4,\mathbb{Q}(\zeta_8))$，因为对于 $i=1,2$，$E_i(\mathbb{Q}(\zeta_{16}))=E_i(\mathbb{Q}(\zeta_8))$。

本文的组织结构如下。第2节致力于研究曲线上的二次点。特别地，我们描述一种算法，在实践中，当曲线 C 的雅可比簇只有有限多个 K-有理点时，该算法可以计算 $\Gamma_2(C,K)$。在第3节中，我们指出，费马¨四次曲线 F_4 在 $\mathbb{Q}$ 上与模曲线 $X_0(64)$ 同构，并回顾 Ozman 和 Siksek 提出的一种方法 [12]，用于确定 $\Gamma_2(X_0(64)\ \mathbb{Q})$。原则上，将 $\mathbb{Q}$ 换成数域 K 后，这种方法很难应用；不过，我们在第5节解释一种受 Mordell 的一个想法启发的技巧，在 $E_1(K)$ 和 $E_2(K)$ 有限的前提下，可以确定 $\Gamma_2(X_0(64)\ K)$。第4节包含本文的另一项重要结果，即命题 6：我们证明，若 E 是定义在 $\mathbb{Q}$ 上的椭圆曲线，且 $j(E)=1728$，那么在任何奇数次数数域中，挠子群 $E(\mathbb{Q})_{\mathrm{tors}}$ 都不会扩大。这一结果对于费马四次曲线上的二次点这一主题之外的研究也有独立价值，并且在定理 1 (ii) 的证明中发挥关键作用。最后，在第6节中，我们给出本文主要结果——定理 1——的证明。附录包含本文中使用的若干亏格一曲线的相关数据。我们还列出若干次数小于 7 且满足定理 1 条件的数域。

本文大量使用计算机代数系统 Magma [4]。用于验证本文计算结论的代码可在 [5]获取。

2. 曲线上的二次点

二次点理论中的一项基本结果如下，它由 Abramovich 和 Harris [1]以及 Harris 和 Silverman [8] 的结果推出（另见 [3]）。

定理 4. 设 C 是定义在数域 K 上的亏格为 $g\geq 2$的曲线。那么， $\Gamma_2(C,K)$ 是无限集，当且仅当 C 在 K 上是超椭圆曲线，或在 K 上是双椭圆曲线，且存在双椭圆映射 $C\to E$，使得椭圆曲线 E 在 K上的秩为正。

对于定义在数域 K 上、亏格为 ≥ 3 且 $J(K)$有限的非超椭圆曲线 C，其中 J 是 C 的雅可比簇，并且至少有一个点 $P_0\in C(K)$，存在一种理论方法，可通过计算次数为 2 的有理有效除子来确定所有二次点。该方法依赖于单射 $\iota: C^{(2)}(K)\to J(K)$，其中 $C^{(2)}$ 表示 C的第二对称积，从而可以从 $J(K)$中的元素恢复二次点。对于每个 $[D]\in J(K)$，计算黎曼-罗赫空间 $\mathcal{L}(D+2P_0)$。若其维数为 1，则可以确定一个次数为 2 的有效除子。然而，计算 $J(K)$往往很困难。即使可行，对于较大的群，所需的黎曼-罗赫计算也可能不切实际。

因此，尽管在理论上是合理的，这种方法计算量很大，而且未必总是切实可行。

在第5节中，我们提出一种比前一种简单得多的方法，该方法基于Mordell的思想，使我们能够确定费马四次曲线在数域上的二次点。

3. A MODULAR APPROACH

值得注意的是，费马四次曲线与非超椭圆的亏格3模曲线 $X_0(64)$是 $\mathbb{Q}$-同构的，并且 E_1 与模曲线 $X_0(32)$是 $\mathbb{Q}$-同构的。

Ozman和Siksek [12] 确定了模曲线 $X_0(N)$上的二次点，其中该曲线是非超椭圆的，亏格为3、4或5，且 $J_0(N)$的Mordell–Weil群是有限的。特别包括模曲线 $X_0(64)$的情形。他们的方法首先确定有理尖点子群 $C_0(64)(\mathbb{Q})$（定义见 [12] ），并界定其在 $J_0(64)(\mathbb{Q})$中的指数，其中 $J_0(64)$是 $X_0(64)$的雅可比簇。由此得到一个正整数 I，使得 $I\cdot J_0(64)(\mathbb{Q})\subseteq C_0(64)(\mathbb{Q})$。因此，有效二次除子 D对某个 $[D']\in J_0(64)(\mathbb{Q})$满足 $[D-2P_0]=I\cdot[D']$。为了细化搜索，他们应用Mordell–Weil筛法的一个版本，以排除 D'的大多数可能性。最后，他们利用Riemann–Roch理论显式确定除子 D。

通过将 $\mathbb{Q}$ 替换为数域 K （其 $J_0(64)(K)$是有限的）来应用这种方法，似乎很自然。尽管理论上这似乎可行，但数域中的计算让我们相信，假设一切都按预期进行，要实现我们的目标并不容易。因此，我们在第5节提出一种简单得多且高效的方法。

引理 5. 我们有 $J_0(64) \overset{\mathbb{Q}}{\sim} E_1^2 \times E_2$。特别地，如果 K 是一个数域，那么 秩$_{\mathbb{Z}}\, J_0(64)(K)$ =2秩$_{\mathbb{Z}}\, E_1(K)$ + 秩$_{\mathbb{Z}}\, E_2(K)$

证明。下表第一列列出了 F_4 中的三个对合及其对应定义。最后一列给出了由这些对合得到的商椭圆曲线。

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

由于 $X_0(64)$ 的亏格为 3，上表表明

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

特别地，$\mathrm{rank}_{\mathbb{Z}}\, J_0(64)(K) = 2\mathrm{rank}_{\mathbb{Z}}\, E_1(K) + \mathrm{rank}_{\mathbb{Z}}\, E_2(K)$ □

4. On torsion growth of elliptic curves.

下面的结果本身也很有意义。它将直接用于推导定理 1 的第二部分。

命题 6. 设 E 是定义在 $\mathbb{Q}$ 上的椭圆曲线，满足 $j(E) = 1728$，且 K 是一个奇数次数域。则 $E(K)_{tors} = E(\mathbb{Q})_{tors}$。

证明. 首先，注意到由于 $j(E) = 1728$，E 与 E_k：$y^2 = x^3 + kx$ 在 $\mathbb{Q}$ 上同构，其中 k 是无四次幂因子的整数（见 [14, 附录 A §3]）。众所周知（见 [13, 命题 6.1(a)]）：

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

证明：若 K 是一个数域，且 $E(K)_{\mathrm{tors}} \neq E(\mathbb{Q})_{\mathrm{tors}}$，则其次数为偶数。为此，只需证明若 $P = (x, y) \in E(\mathbb{Q})_{\mathrm{tors}}$，其中 $P \notin E(\mathbb{Q})$，则 $[\mathbb{Q}(P):\mathbb{Q}]$ 为偶数，其中 $\mathbb{Q}(P) = \mathbb{Q}(x, y)$。具体而言，只需考虑 P 的奇数素数阶情形或 2 的幂阶情形。

设 p 是一个素数，$G_E(p)$ 是 E 的 p-挠点上的模 p 伽罗瓦表示的像（在 $\mathrm{GL}_2(\mathbb{F}_p)$ 中相差一个共轭）。在复乘法情形下，$G_E(p)$ 的可能情况已完全为人所知；这要归功于 Zywina 的工作 [17, §1.9]。由于 $j(E) = 1728$，E 具有复乘法，乘子为 $\mathbb{Z}[\sqrt{-1}]$，并且我们有

- $p = 2$，则 $G_E(p)$ 是 $B(2)$ 或 $C_s(2)$，
- $p \equiv 1$（模 4），则 $G_E(p)$ 是 $C_{ns}^+(p)$ 或 $\mathrm{GL}_2(\mathbb{F}_p)$，
- $p \equiv 3$（模 4），则 $G_E(p)$ 是 $C_s^+(p)$ 或 $\mathrm{GL}_2(\mathbb{F}_p)$，

其中，$B(p)$（分别为 $C_s(p)$、$C_{ns}(p)$）表示 $\mathrm{GL}_2(\mathbb{F}_p)$ 的 Borel 子群（分别为分裂 Cartan 子群、非分裂 Cartan 子群），而 $C_s^+(p)$（分别为 $C_{ns}^+(p)$）是 $\mathrm{GL}_2(\mathbb{F}_p)$ 中 $C_s(p)$（分别为 $C_{ns}(p)$）的正规化子。

设 p 为素数，且 $P \in E[p]$ 是椭圆曲线 E上的一个 p 阶点。那么，[6, 定理 5.6] 给出了 $[\mathbb{Q}(P):\mathbb{Q}]$ 可能取到的次数，具体取决于 $G_E(p)$。在特殊情形 $j(E) = 1728$下，我们有

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

因此，若 p 是奇素数，则 $[\mathbb{Q}(P):\mathbb{Q}]$ 为偶数。

为完成证明，设 P 是一个阶为 2 的幂、且未定义在 $\mathbb{Q}$ 上的点。由 [6,定理 4.6] 可知，$[\mathbb{Q}(P):\mathbb{Q}(2P)]$ 整除 2。特别地，这证明了 $[\mathbb{Q}(P):\mathbb{Q}]$ 是偶数，因为 E 中的 2 阶点定义在 $\mathbb{Q}$ 上，或定义在某个二次数域上。□

5. A Procedure Inspired by Mordell's approach

本节中，给定一个数域 K，我们给出一个步骤，用于确定集合 $S_2^0(F_4,\ K)$，前提是已知集合 $E_1(K)$ 和 $E_2(K)$。

设 $L=K(\sqrt{d})$ 是 K 的二次扩张，其中 $d\in K$ 满足 $d\notin K^2$。由于 $x\neq 0$、$y^2\neq\pm 1$ 和 $x^4+y^4=1$，我们有 $(1+y^2)/x^2=x^2/(1-y^2)$。令

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

通过直接计算可验证 $t\notin\{0,\pm 1,\pm\zeta_8^2\}$。由 $x^4+y^4=1$ 和 (1) 可直接得到

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

设 $s=2t$、$2u=x(s^2+4)$ 和 $2v=xy(s^2+4)$。由 (2) 可推出

$$\begin{aligned} E_1&:\ u^2=s^3+4s,\\ E_2&:\ v^2=s^3-4s. \end{aligned} \tag{3}$$

我们将根据 $t\in K$ 是否成立，把步骤分为两部分。

- **步骤 I:** $t\in K$. 设 $u=a_1+b_1\sqrt{d}$ 和 $v=a_2+b_2\sqrt{d}$，其中 $a_1,\ a_2,\ b_1,\ b_2\in K$. 由 (3) 得，$u^2,\ v^2\in K$. 由于 $\sqrt{d}\notin K$, $a_1b_1=a_2b_2=0$. 我们考虑以下几种情况:
  - $b_1=0$. 那么 $u=a_1\in K$. 因此 $(s,\ u)\in E_1(K)$.
  - $b_2=0$. 那么 $v=a_2\in K$. 因此 $(s,\ v)\in E_2(K)$.
  - $b_1b_2\neq 0$. 那么 $a_1=a_2=0$. 由 (3) 可得

$$\begin{aligned} db_1^2&=s(s^2+4),\\ db_2^2&=s(s^2-4). \end{aligned}$$

因此,

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

其中 $r=db_1b_2v/s\in K$。因此 $(s,\ r)\in H_3(K)$。注意，曲线 H_3 可通过映射与E_1 作 $\mathbb{Q}$-同构:

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

在这一步骤中，我们需要计算曲线 E_1、E_2 和H_3上的 K-有理点。由每个点的第一个坐标，我们得到 s，随后计算 x^2 和 y^2，最后计算 $(x,\ y)\in S_2^0(F_4,\ K)$。

- **第二步:** $t\notin K$。令 $Q(T)\in K[T]$为 s在 K上的首一最小多项式。由于 $[L:\ K]=2$和 $t\notin K$，因此 $\deg Q(T)=2$ 且 $L=K(s)$。根据 (3)，存在 $\alpha_1,\ \alpha_2,\ \beta_1,\ \beta_2\in K$ 使得

$$\begin{aligned} s^3+4s&=(\alpha_1+\beta_1 s)^2,\\ s^3-4s&=(\alpha_2+\beta_2 s)^2. \end{aligned}$$

因此，存在 $r_1,\ r_2\in K$ 使得

$$\begin{aligned} T^3+4T-(\alpha_1+\beta_1T)^2&=Q(T)\,(T-r_1)\,,\\ T^3-4T-(\alpha_2+\beta_2T)^2&=Q(T)\,(T-r_2)\,. \end{aligned}$$

因此，对于 $j=1,\ 2$，$(r_j,\alpha_j+\beta_jr_j)\in E_j(K)$。对于 $P_j=(x_j,y_j)\in E_j(K)$，设 $Q_{\beta_j}(T)\in K[T]$, $j=1,2$，使得

$$\begin{aligned} T^3+4T-(y_1-\beta_1x_1+\beta_1T)^2&=Q_{\beta_1}(T)\,(T-x_1)\,,\\ T^3-4T-(y_2-\beta_2x_2+\beta_2T)^2&=Q_{\beta_2}(T)\,(T-x_2)\,. \end{aligned}$$

注意，对于 $j=1,2$，将 P_j 替换为 $-P_j$ 等价于将 β_j 替换为 $-\beta_j$。因此，我们只需实现每个集合 $\{\pm P_j\}$ 中各取一个元素的计算。

最后，我们通过求解由等式$Q_{\beta_1}(T)=Q_{\beta_2}(T)$得到的二次方程组，进而求出 $\beta_1,\ \beta_2\in K$；然后求出 $s=t/2$ 在 K 上的最小多项式 $Q(T)$。也就是说，我们得到 s，随后计算 x^2 和 y^2，最后得到$(x,\ y)\in S_2^0(F_4,\ K)$。

6. Proof of Theorem 1

定理 1 的证明 (i)。 在第5节中，给定一个数域 K，我们给出了一个步骤，可由 $E_1(K)$和 $E_2(K)$中的点计算 $\Gamma_2(F_4,\ K)$。在秩$_{\mathbb{Z}}\, E_j(K)\ = 0, j = 1,\ 2$ 的特殊情形下，这些集合都是有限的，因此 $\Gamma_2($ $F_4,\ K)$也是有限的。这就证明了定理 1 的第一部分。

另一种证明来自定理 4，以及引理 5 中所确立的 F_4 的雅可比簇分解。

定理 1 的证明 (ii)。注意到 $j(E_1)\ = j(E_2)\ = 1728$，因此，若 K 是奇数次数域，则命题 6 断言 $E_j(K)_{\mathrm{tors}} = E_j(\mathbb{Q})_{\mathrm{tors}}, j = 1,2$。此外，在秩$_{\mathbb{Z}} E_j(K)\ = 0$ 的特殊情形下，我们有 $E_j(K)\ = E_j(\mathbb{Q}),$ $j\ = 1,2$。定理 1(ii) 可由第 5 节所述步骤推出。也就是说， $\Gamma_2(F_4, K)\ = \Gamma_2(F_4, \mathbb{Q})$。

定理 1(iii) 的证明。设 K 是一个数域，使得秩$_{\mathbb{Z}}\, E_j(K)\ = 0, j = 1, 2$。然后，第 5 节给出的步骤可以利用 $E_1(K)_{\mathrm{tors}}$ 和 $E_2(K)_{\mathrm{tors}}$ 的点来计算 $\Gamma_2(F_4, K)$。特别地，若 L 是包含在 K 中的最大子域，且满足 $E_j(K)_{\mathrm{tors}} = E_j(L)_{\mathrm{tors}}$，其中 $j\ = 1, 2$，则 $\Gamma_2(F_4, K)\ = \Gamma_2(F_4, L)$。这将研究范围限定为挠点在 E_1 和／或 E_2 中增长的数域。附录中证明了这类域为 $\mathbb{Q}(\sqrt{-1})$、 $\mathbb{Q}(\sqrt{2})$、$\mathbb{Q}(\zeta_8)$和 $\mathbb{Q}(\alpha)$,⁻ 其中 α 满足 $\alpha^4 - 2\alpha^2 - 1 = 0$。注意，对于这些域，椭圆曲线 E_1 和 E_2 的秩均为 0。因此，只需计算这些域上的 $\Gamma_2(F_4, K)$ 和 $\Gamma_2(F_4, \mathbb{Q})$。为此，附录提供了这些数域 K 中各点所需的数据。

步骤 I. $E_1(K)$ $E_2(K)$ 和 $H_3(K)$ 中的仿射点。

第二步. 我们给出一个表，对于每一对点 (P_1, P_2)、 $P_1 \in E_1(K)$ 和 $P_2 \in E_2(K)$，如果在 K 中不存在解 (β_1, β_2)，或者相应的二次多项式 $Q(x)$ 可约，或者 $t \in \{0, \pm1, \pm\sqrt{-1}\}$，则显示符号 ✗ 。否则，显示 s 的相应不可约二次极小多项式 $Q(x)$ 以及 $S_2^0(F_4, K)$ 中的点。

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

$$E_1(\mathbb{Q}) = \{(0, 0), (2, \pm4), [0 : 1 : 0]\},$$
$$E_2(\mathbb{Q}) = \{(0, 0), (\pm2, 0), [0 : 1 : 0]\},$$
$$H_3(\mathbb{Q}) = \{(\pm2, 0), [1 : \pm1 : 0]\}.$$

步骤 I. 对于 s 的每个取值，我们得到 $\Gamma_2(F_4, \mathbb{Q})$ 中的以下点:

s	$(x,\ y) \in \Gamma_2(F_4,\ \mathbb{Q}))$	b 在 $\mathbb{Q}$ 上的最小多项式
0	$(0, b)$	$T^2 + 1$
2	$(1, 0)$	$T - 1$
-2	$(b, 0)$	$T^2 + 1$

注意， $\Gamma_2(F_4, \mathbb{Q})$中的那些点是平凡点。

第二步 我们确定如下表格

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

因此， $S_2^0(F_4,\mathbb{Q}) = \{(\omega,\omega)\}$，其中 $\omega = (1+\sqrt{-7})/2$ 和 $\omega = (1-\sqrt{-7})/2$。

至此完成了对 $\Gamma_2(F_4,\ K)$ 的计算证明。特别地，我们证明了：若 F_4 在二次数域 $\mathbb{Q}(\sqrt{d})$ 中有非平凡点，则 $d=-7$，这正是 Aigner 的结果（参见 [2]）。

6.2. $\Gamma_2(F_4,\ \mathbb{Q}(\sqrt{-1}))$。那么 $K=\mathbb{Q}(\sqrt{-1})$ 并且

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

步骤 I。对于 $s \notin \mathbb{Q}$ 的每个取值，我们计算 $\Gamma_2(F_4,\ \mathbb{Q}(\sqrt{-1}))$ 中的以下各点：

s	$(x,\ y) \in \Gamma_2(F_4,\ \mathbb{Q}(\sqrt{-1}))$	b 在 $\mathbb{Q}$ 上的最小多项式
$2\sqrt{-1}$	$(-b,\ 1)$	$T^2+\sqrt{-1}$
$-2\sqrt{-1}$	$(-b,\ 1)$	$T^2-\sqrt{-1}$

注意，$\Gamma_2(F_4,\ \mathbb{Q}(\sqrt{-1}))$ 中的那些点是平凡点。

第二步。我们计算出以下表格

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

因此，$S_2^0(F_4,\mathbb{Q}(\sqrt{-1})) = \{\sqrt{-1}(\omega,\omega),\ (\sqrt{-1}\omega,\omega),\ (\omega,\sqrt{-1}\omega)\}$。这就完成了对 $\Gamma_2(F_4,\mathbb{Q}(\sqrt{-1}))$ 的计算证明。

6.3. $\Gamma_2(F_4,\mathbb{Q}(\sqrt{2}))$。那么 $K=\mathbb{Q}(\sqrt{2})$ 和

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

步骤 I. 对于每个 $s \notin \mathbb{Q}$ 的取值，我们在 $\Gamma_2(F_4,\mathbb{Q}(\sqrt{2}))$ 中得到以下点：

s	$(x,\ y) \in \Gamma_2(F_4,\ \mathbb{Q}(\sqrt{2}))$	b 在 $\mathbb{Q}$ 上的最小多项式
$2\sqrt{2}+2$	$(-b,\ -b)$	$T^2-1/2\sqrt{2}$
$-2\sqrt{2}+2$	$(-b,\ -b)$	$T^2+1/2\sqrt{2}$

我们确定 $S_2^0(F_4,\mathbb{Q}(\sqrt{2}))$ 中的点 $(1/\sqrt[4]{2}, 1/\sqrt[4]{2})$ $\sqrt{-1}(1/\sqrt[4]{2}, 1/\sqrt[4]{2})$。

第二步。 我们计算如下表

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

因此， $S_2^0(F_4,\mathbb{Q}(\sqrt{2})) = \{(1/\sqrt[4]{2}, 1/\sqrt[4]{2})\ \sqrt{-1}(1/\sqrt[4]{2}, 1/\sqrt[4]{2})\}$。至此， $S_2^0(F_4,\mathbb{Q}(\sqrt{2}))$ 的计算证明完成。

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

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

Step I. 对于 $s \notin \mathbb{Q}(\sqrt{2})$ 的每个取值，我们确定 $\Gamma_2(F_4,\mathbb{Q}(\alpha))$ 中的以下点 :

s	$(x,\ y) \in \Gamma_2(F_4,\ \mathbb{Q}(\alpha))$	b在 $\mathbb{Q}(\alpha)$上的最小多项式
-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	$(b,\ -\alpha^3+2\alpha)$	$T^2+\alpha^3-3\alpha$
$2\alpha^3+2\alpha^2-2\alpha$	$(-\alpha^3+2\alpha,\ b)$	$T^2+\alpha^3-3\alpha$

我们得到点 $(\delta, -\alpha^3+2\alpha)$, $(\sqrt{-1}\delta, -\alpha^3+2\alpha)$, 它们位于 $S_2^0(F_4,\mathbb{Q}(\alpha))$ 中，其中 δ满足 $\delta^2=\alpha^3-3\alpha$。**第二步**。 我们计算得到下表

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

第二步没有产生新的点。因此,

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

这就完成了对 $\Gamma_2(F_4,\mathbb{Q}(\alpha))$ 的计算证明。

6.5. $\Gamma_2(F_4, \mathbb{Q}(\zeta_8))$。于是 $K = \mathbb{Q}(\zeta_8)$ 和

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

步骤 I. 对于 $s \notin \mathbb{Q}(\sqrt{-1}) = \mathbb{Q}(\zeta_8^2)$ 和 $s \notin \mathbb{Q}(\sqrt{2}) = \mathbb{Q}(\zeta_8^3 - \zeta_8)$ 的每个取值，我们推导出 $\Gamma_2(F_4, \mathbb{Q}(\zeta_8))$ 中的以下点：

s	$(x,\ y) \in \Gamma_2(F_4,\ \mathbb{Q}(\zeta_8))$	b 在 $\mathbb{Q}(\zeta_8)$ 上的最小多项式
$2\zeta_8$	$(-b,\ -\zeta_8)$	$T^2 + \sqrt{2}$
$-2\zeta_8^3 - 2\zeta_8^2 - 2\zeta_8$	$(-\zeta_8,\ -b)$	$T^2 + \sqrt{2}$
$-2\zeta_8^3$	$(-b,\ -\zeta_8^3)$	$T^2 + \sqrt{2}$
$2\zeta_8^3 + 2\zeta_8^2 + 2\zeta_8$	$(-\zeta_8^3,\ -b)$	$T^2 + \sqrt{2}$
$-2\zeta_8$	$(-b,\ -\zeta_8)$	$T^2 - \sqrt{2}$
$2\zeta_8^3 - 2\zeta_8^2 + 2\zeta_8$	$(-\zeta_8,\ -b)$	$T^2 - \sqrt{2}$
$2\zeta_8^3$	$(-b,\ -\zeta_8^3)$	$T^2 - \sqrt{2}$
$-2\zeta_8^3 + 2\zeta_8^2 - 2\zeta_8$	$(-\zeta_8^3,\ -b)$	$T^2 - \sqrt{2}$
$2\zeta_8^3 - 2\zeta_8 - 2$	$(-b,\ -\zeta_8^2 b)$	$T^2 + 1/2(-\zeta_8^3 + \zeta_8)$
$-2\zeta_8^3 + 2\zeta_8 - 2$	$(-b,\ -\zeta_8^2 b)$	$T^2 + 1/2(\zeta_8^3 - \zeta_8)$

我们得到 $S_2^0(F_4, \mathbb{Q}(\zeta_8))$ 中的点 $(\zeta_8, \sqrt[4]{2})$、$(\zeta_8^3, \sqrt[4]{2})$、$(\zeta_8, \zeta_8^2\sqrt[4]{2})$、$(\zeta_8^3, \zeta_8^2\sqrt[4]{2})$ 和 $(1/\sqrt[4]{2}, \zeta_8^2/\sqrt[4]{2})$。

第二步。 我们计算表1。在下表中，对于每一对点 $P_j \in E_j(\mathbb{Q}(\zeta_8))$，$j = 1,\ 2$，如果表1中相应位置不是✗，且它在 $\mathbb{Q}(\zeta_8)$ 中是本原的，我们将 $S_2^0(F_4,\ \mathbb{Q}(\zeta_8))$ 中的相应点化简为：

$(1/4(-\zeta_8^3 + \zeta_8)s + 1/2(-\zeta_8^3 + \zeta_8)\ \ 1/4(-\zeta_8^3 + \zeta_8)s + 1/2(\zeta_8^3 + \zeta_8))$ $s^2 + (2 + 2\zeta_8^2)s - 4\zeta_8^2 = 0$	$(\zeta_3\zeta_8^3,\ -\zeta_3^2\zeta_8^3)$
$(1/4(-\zeta_8^3 + \zeta_8)s + 1/2(-\zeta_8^3 + \zeta_8)\ \ 1/4(-\zeta_8^3 + \zeta_8)s + 1/2(-\zeta_8^3 - \zeta_8))$ $s^2 + (-2\zeta_8^2 + 2)s + 4\zeta_8^2 = 0$	$(-\zeta_3^2\zeta_8,\ \zeta_3\zeta_8)$
$(1/4(-\zeta_8^3 - \zeta_8)s + 1/2(\zeta_8^3 + \zeta_8)\ \ 1/4(-\zeta_8^3 + \zeta_8)s + 1/2(\zeta_8^3 + \zeta_8))$ $s^2 + (2\zeta_8^2 - 2)s + 4\zeta_8^2 = 0$	$(-\zeta_3\zeta_8^3,\ -\zeta_3^2\zeta_8)$
$(1/4(-\zeta_8^3 - \zeta_8)s + 1/2(\zeta_8^3 + \zeta_8)\ \ 1/4(-\zeta_8^3 + \zeta_8)s + 1/2(-\zeta_8^3 - \zeta_8))$ $s^2 + (-2\zeta_8^2 - 2)s - 4\zeta_8^2 = 0$	$(-\zeta_3^2\zeta_8,\ \zeta_3\zeta_8^3)$

$(1/8(-\zeta_8^2+1)s+1/4(-\zeta_8^2-3)\ 1/8(-\zeta_8^3-\zeta_8)s+1/4(3\zeta_8^3+3\zeta_8))$ $s^2+(-6\zeta_8^2-6)s+4\zeta_8^2=0$	$\omega^{-1}(-\zeta_8^2,\ -\overline{\omega}\zeta_8)$
$(1/8(-\zeta_8^2+1)s+1/4(-3\zeta_8^2-1)\ 1/8(-\zeta_8^3-\zeta_8)s+1/4(-3\zeta_8^3-3\zeta_8))$ $s^2+(-6\zeta_8^2+6)s-4\zeta_8^2=0$	$\overline{\omega}^{-1}(-1,\omega\zeta_8^3)$
$(-1/2\zeta_8 s+1/2\zeta_8^3,-1/2\zeta_8^2 s+1/2)$ $s^2+\zeta_8^2 s-2=0$	$\omega^{-1}(-\omega\zeta_8^3,\ 1)$
$(-1/4\zeta_8^3 s+\zeta_8,\ -1/4s)$ $s^2+2\zeta_8^2 s-8=0$	$\overline{\omega}^{-1}(-\omega\zeta_8,\ \zeta_8^2)$
$(1/8(-\zeta_8^2-1)s+1/4(-\zeta_8^2+3)\ 1/8(-\zeta_8^3-\zeta_8)s+1/4(3\zeta_8^3+3\zeta_8))$ $s^2+(6\zeta_8^2-6)s-4\zeta_8^2=0$	$\overline{\omega}^{-1}(-\zeta_8^2,-\omega\zeta_8^3)$
$(1/8(-\zeta_8^2-1)s+1/4(-3\zeta_8^2+1)\ 1/8(-\zeta_8^3-\zeta_8)s+1/4(-3\zeta_8^3-3\zeta_8))$ $s^2+(6\zeta_8^2+6)s+4\zeta_8^2=0$	$\omega^{-1}(1,\overline{\omega}\zeta_8)$
$(-1/4\zeta_8 s+\zeta_8^3,\ -1/4s)$ $s^2-2\zeta_8^2 s-8=0$	$\omega^{-1}(-\omega\overline{\zeta}_8^3,\ -\zeta_8^2)$
$(-1/2\zeta_8^3 s+1/2\zeta_8,\ -1/2\zeta_8^2 s-1/2)$ $s^2-\zeta_8^2 s-2=0$	$\omega^{-1}(-\omega\overline{\zeta}_8,\ -1)$

我们得到 $S_2^0(F_4,\ \mathbb{Q}(\zeta_8))$ 中的以下各点:

$$(\zeta_3\zeta_8,\zeta_3^2\zeta_8),\quad (\zeta_3\zeta_8^3,\zeta_3^2\zeta_8^3),\quad (\zeta_3\zeta_8,\zeta_3^2\zeta_8^3),\quad (\zeta_3\zeta_8^3,\zeta_3^2\zeta_8),$$
$$\omega^{-1}(\overline{\omega}\zeta_8,1),\quad \omega^{-1}(\overline{\omega}\zeta_8^3,1),\quad \omega^{-1}(\overline{\omega}\zeta_8,\zeta_8^2),\quad \omega^{-1}(\overline{\omega}\zeta_8^3,\zeta_8^2),$$
$$\overline{\omega}^{-1}(\omega\zeta_8,1),\quad \overline{\omega}^{-1}(\omega\zeta_8^3,1),\quad \overline{\omega}^{-1}(\omega\zeta_8,\zeta_8^2),\quad \overline{\omega}^{-1}(\omega\zeta_8^3,\zeta_8^2).$$

这完成了对 $S_2^0(F_4,\ \mathbb{Q}(\zeta_8))$ 的计算，特别也完成了对 $\Gamma_2(F_4,\ \mathbb{Q}(\zeta_8))$ 的计算。

定理 1 的证明 (iv)。 这是第5节中所述方法的直接推论，该方法通过集合 $E_i(K)=E_i(L)$ 计算 $\Gamma_2(F_4,\ K)$，其中 $i=1,\ 2$。

$(-2\sqrt{-1}, 0)$	$R_{1,1}$	$R_{1,2}$	$R_{1,3}$	$R_{1,4}$
✗	✗	✗	✗	✗
$-\zeta_8^3+\zeta_8)s+1/2(-\zeta_8^3+\zeta_8)$, $\zeta_8^3+\zeta_8)s+1/2(-\zeta_8^3-\zeta_8))$ $^2+(-2\zeta_8^2+2)x+4\zeta_8^2$	✗	✗	✗	✗
$-\zeta_8^3-\zeta_8)s+1/2(\zeta_8^3+\zeta_8)$, $-\zeta_8^3+\zeta_8)s+1/2(-\zeta_8^3-\zeta_8))$ $^2+(-2\zeta_8^2-2)x-4\zeta_8^2$	✗	✗	✗	✗
$-1/4\zeta_8^3 s+\zeta_8,-1/4s)$ $x^2+2\zeta_8^2 x-8$	✗	✗	✗	✗
$\zeta_8^3 s+1/2\zeta_8,-1/2\zeta_8^2 s-1/2)$ $x^2-\zeta_8^2 x-2$	✗	✗	✗	✗
✗	✗	✗	✗	✗
✗	✗	✗	✗	✗
✗	✗	✗	✗	✗
✗	✗	✗	✗	✗

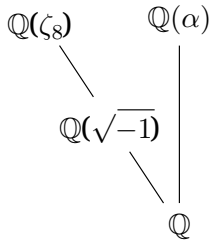
APPENDIX

在第5节中，我们介绍了一个步骤：给定一个数域 K，满足 $E_1(K)$和 $E_2(K)$均为有限集，该步骤可以确定 $\Gamma_2(F_4,\ K)$。因此，问题归结为确定 E_1 和 E_2 在数域上的挠增长。注意，E_2 是 E_1的 -1-扭曲。特别地，它们在 $\mathbb{Q}(\zeta_8)$上同构。令

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

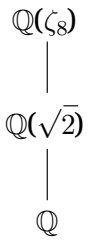
下表展示了椭圆曲线 E_1 在次数小于8的情况下的挠增长信息。这些信息是从[1] LMFDB 数据库 [15], 中获得的，其中 E_1 的 LMFDB 标签为32.a4。每一行的第二列显示第一列所列数域 K 上的挠点结构。第三列显示 $E_1(K)_{\text{tors}}$ 中不来自任意真子域 K' 上的 $E_1(K')_{\text{tors}}$ 的点，其中 K' 是 K的真子域。表格右侧展示了一个图，其中列出了参与 E_1挠增长的所有数域（次数为 <8）。注意，α 满足 $\alpha^4-2\alpha^2-1=0$。

K	$E_1(K)_{\text{tors}}$	数据 $E_1(K)_{\text{tors}}$
$\mathbb{Q}$	$\mathbb{Z}/4\mathbb{Z}$	$(0,0),\ \pm(2,4)$
$\mathbb{Q}(\sqrt{-1})$	$\mathbb{Z}/2\mathbb{Z}\oplus\mathbb{Z}/4\mathbb{Z}$	$\pm(-2,\ -4\sqrt{-1}),\ (\pm2\sqrt{-1},\ 0)$
$\mathbb{Q}(\zeta_8)$	$\mathbb{Z}/4\mathbb{Z}\oplus\mathbb{Z}/4\mathbb{Z}$	$\pm R_{1,1},\ \pm R_{1,2},\ \pm R_{1,3},\ \pm R_{1,4}$
$\mathbb{Q}(\alpha)$	$\mathbb{Z}/8\mathbb{Z}$	$\pm S_{1,1},\ \pm S_{1,2}$

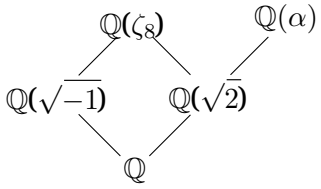


同样，对于椭圆曲线 E_2，考虑到其 LMFDB 标签为 64.a3。

K	$E_2(K)_{\text{tors}}$	数据 $E_2(K)_{\text{tors}}$
$\mathbb{Q}$	$\mathbb{Z}/2\mathbb{Z}\oplus\mathbb{Z}/2\mathbb{Z}$	$(0,0),(\pm2,0)$
$\mathbb{Q}(\sqrt{2})$	$\mathbb{Z}/2\mathbb{Z}\oplus\mathbb{Z}/4\mathbb{Z}$	$\pm(2(\sqrt{2}+1),4(\sqrt{2}+1))$ $\pm(2(-\sqrt{2}+1),4(\sqrt{2}-1))$
$\mathbb{Q}(\zeta_8)$	$\mathbb{Z}/4\mathbb{Z}\oplus\mathbb{Z}/4\mathbb{Z}$	$\pm R_{2,1}, \pm R_{2,2}, \pm R_{2,3},\ \pm R_{2,4},\ \pm R_{2,5},\ \pm R_{2,6}$



下图展示了与椭圆曲线 E_1 和 E_2的挠点增长相关的数域格：



一些计算。 在本节中，我们展示一些满足应用定理 1 所需条件的数域。

[1]挠增长数据由作者和 Filip Najman 计算得出[7]。

以下列表列出了所有满足条件 $\operatorname{rank}_{\mathbb{Z}} E_1(\mathbb{Q}(\sqrt{D})) = \operatorname{rank}_{\mathbb{Z}} E_2(\mathbb{Q}(\sqrt{D}) = 0$ 的无平方因子整数 $D \neq -1,\ 2,\ |D| < 200$:

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

下表展示了五个数域的定义多项式 K，使得对于 $[K$，有 $\operatorname{rank}_{\mathbb{Z}} E_1(K) = \operatorname{rank}_{\mathbb{Z}} E_2(K) = 0 :\ \mathbb{Q}] = d$，满足 $d = 3,4,5$。

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

对于次数为 6 或 7 的情形，我们仅能找到数域 $\mathbb{Q}(\delta)$，其 δ 的最小多项式为 $x^6 - x^4 - 2x^3 + 2x + 1$，且满足应用定理 1 所需的条件。在我们尝试证明秩$_{\mathbb{Z}} E_j(K) = 0\ j = 1,\ 2$ 的大多数数域中，Magma 都无法执行计算。因此，我们选择计算解析秩，但也未能成功。最后，我们尝试确定 $L(E_1/K,\ 1)$ 和$L(E_2/K,\ 1)$ 是否为零。然而，这种方法也未能找到满足应用定理 1 所需条件的新数域。

References

[1] D. Abramovich 和 J. Harris，$W_d(C)$ 中的阿贝尔簇与曲线，Compositio Math. 78 (1991), 227-238。[2] A. Aigner，¨关于在二次¨域中 $x^4 + y^4 = z^4$ 的可能性，*J. Math. Verein.*, 43 (1934), 226-228。[3] F. Bars，经典模曲线上的二次点。Momose 纪念文集。与模曲线相关的数论。Contemp. Math. 701 (2018), 17-34。[4] W. Bosma、J. Cannon 和 C. Playoust，MAGMA 代数系统。I. 用户语言，*J. Symbolic Comput.*, 24 3 4 1997 235 265 : - ( ), - . [5] E. Gonz´alez-Jim´enez，数域上的费马四次曲线的二次点。Magma 源代码。https://www.uam.es/enrique.gonzalez.jimenez/. [6] E. Gonz´alez-Jim´enez 和 F. Najman，基变换下椭圆曲线挠点的增长，Math. Comp. 89 (2020), 1457–1485。[7] E. Gonz´alez-Jim´enez 和 F. Najman，确定椭圆曲线挠增长的算法，Exp. Math. 32 (2023), 70–81。[8] J. Harris 和 J. H. Silverman，双椭圆曲线与对称积，Proc. Amer. Math. Soc. 112 (1991) 347-356。[9] Y. Ishitsuka、T. Ito 和 T. Oshita，费马四次曲线相关的模 4 伽罗瓦表示的显式计算，*Int. J. Number Theory*, 16: 4 (2020), 881-905。[10] M. Khawaja 和 F. Jarvis，在 $\mathbb{Q}\ \sqrt{2}\ \sqrt{3}$ 14 2025 19, (,) 457 480 上的费马大定理，Algebra Number Theory ( ), no. – .[11] L. J. Mordell，代数数域中的丢番图方程 $x^4 + y^4 = 1$，*Acta Arith.*, 14 (1967/1968), 347-355。[12] E. Ozman 和 S. Siksek，模曲线上的二次点。Math. Comp. 88 (2019), 2461-2484。[13] J. H. Silverman，*The arithmetic of elliptic curves*，Graduate Texts in Mathematics，第 106 卷。Springer，多德雷赫特，第二版 (2009)。[14] J. H. Silverman，*Advanced topics in the arithmetic of elliptic curves*，Graduate Texts in Mathematics，第 151 卷，Springer-Verlag，纽约 (1994)。[15] LMFDB 协作组，L-函数与模形式数据库，https://www.lmfdb.org，2024, [在线；访问于 2024] 年 7 月 15 日。[16] N.X. Tho，*Points on $x^4 + y^4 = z^4$ over quadratic extensions of $\mathbb{Q}(\zeta_8)(T_1, \ldots, T_n)$*。Bull. Aust. Math. Soc. 111 (2025), 19–31。[17] D. Zywina，椭圆曲线在 $\mathbb{Q}$上相关的模 ℓ 表示可能出现的像。https://arxiv.org/abs/1508.07660

Universidad Autónoma de Madrid, Departamento de Matemáticas, Madrid, Spain
Email address: enrique.gonzalez.jimenez@uam.es