arXiv:2602.01384v1 [math.NT] 1 Feb 2026

关于具有同源的椭圆曲线判别式的平方性

´ ´ENRIQUE GONZALEZ-JIMENEZ

Abstract. 我们对满足以下条件的 N 取值进行了分类：定义在$\mathbb{Q}$ 上的椭圆曲线具有平方判别式，并且存在一个 N-同源。此外，我们还确定了这样的 N 取值：定义在 $\mathbb{Q}$ 上的两条椭圆曲线均具有平方判别式，且彼此 N-同源。在这两种情形下，我们都明确地参数化了与这些问题相关的椭圆曲线的 j 不变量。

1. Introduction

设 E 是定义在 $\mathbb{Q}$上的椭圆曲线，其魏尔斯特拉斯方程为

$$E\colon y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

E 的判别式记作 $\Delta(E)$，它由系数 a_1，a_2，a_3，a_4，a_6 定义（见 [8,第三章.1]）。 E 的任何其他魏尔斯特拉斯方程均可通过以下变量变换得到

$$\begin{aligned} x &= u^2x' + r,\\ y &= u^3y' + u^2sx' + t, \end{aligned}$$

其中 u，r，s，$t \in \mathbb{Q}$ 以及 $u \neq 0$。若 E' 表示由这种变换后的方程所定义的曲线，则它们的判别式满足

$$\Delta(E) = u^{12}\Delta(E').$$

因此， $\Delta(E)$ 在 $\mathbb{Q}$ 中为平方这一性质是椭圆曲线 E 本身固有的，并不取决于所选的魏尔斯特拉斯方程。换言之，陈述 $\sqrt{\Delta(E)} \in \mathbb{Q}$ 是曲线本身的性质。

本文旨在系统地分类：在特定族中，椭圆曲线的判别式为完全平方的条件。理解这一性质至关重要，因为它对椭圆曲线的算术有重要影响。

在 [3], 中，我们通过分析挠子群的结构来研究这一问题。具体而言，前述工作的一项主要结果证明，若 E 是定义在 $\mathbb{Q}$ 上的椭圆曲线，且 $\sqrt{\Delta(E)} \in \mathbb{Q}$，则 $|E(\mathbb{Q})_{\mathrm{tors}}| \in \{1, 3\}$ 或 $E(\mathbb{Q})_{\mathrm{tors}}$ 是非循环的。然而，只有当 $E(\mathbb{Q})_{\mathrm{tors}}$ 是非循环的情况下，逆命题才成立。本文将重点研究定义在 $\mathbb{Q}$ 上且存在定义在 $\mathbb{Q}$上的（循环）同源的椭圆曲线。全文采用如下约定：同源椭圆曲线视为非同构。

本文的主要结果如下三个定理所述。

定理 1. 设 E 是定义在 $\mathbb{Q}$ 上的椭圆曲线，使得 $\sqrt{\Delta(E)} \in \mathbb{Q}$。若 E 具有一条 N-同源，则 $N \in \{2, 3, 4, 6, 7, 8\}$。下表给出 E的 j-不变量的参数化：

Date：2026年2月3日。2020 *Mathematics Subject Classification.* 主要分类号：11G05，次要分类号：14H52。作者获得了由MCIN/AEI/10.13039/501100011033资助的项目PID2022-138916NB-I00的支持，该项目由欧洲区域发展基金“建设欧洲之道”提供资金。

N	$j(E)$
2	$\frac{256(t^2+t+1)^3}{t^2(t+1)^2}$
3	$\frac{(t^2+3)^3(t^2+27)}{t^2}$
4	$\frac{256(t^4+4t^3+5t^2+2t+1)^3}{t^2(t+1)^4(t+2)^2}$
6	$\frac{256(t^2+3t+3)^3(t^6+9t^5+30t^4+45t^3+30t^2+9t+3)^3}{t^2(t+1)^6(t+2)^6(t+3)^2(2t+3)^2}$
7	$\frac{(t^2-t+7)(t^2+t+7)(t^4+5t^2+1)^3}{t^2}$
8	$\frac{256(t^8+8t^7+28t^6+56t^5+69t^4+52t^3+22t^2+4t+1)^3}{t^2(t+1)^8(t+2)^2(t^2+2t+2)^2}$

定理 2. 设 E 和 E' 是定义在 $\mathbb{Q}$ 上的两条椭圆曲线，使得 $\sqrt{\Delta(E)}\ \sqrt{\Delta(E')}\ \in \mathbb{Q}$。若 E和 E' 是 N-同源的，则 $N \in \{2,3,4,7\}$。下表给出了 E 和 E'的 j-不变量的参数化：

N	$j(E)$	$j(E')$
2	$\frac{256(t^4-t^2+1)^3}{(t-1)^2t^4(t+1)^2}$	$\frac{16(t^4+14t^2+1)^3}{(t-1)^4t^2(t+1)^4}$
3	$\frac{(t^2+3)^3(t^2+27)}{t^2}$	$\frac{(t^2+27)(t^2+243)^3}{t^6}$
4	$\frac{256(t^8-t^4+1)^3}{(t-1)^2t^8(t+1)^2(t^2+1)^2}$	$\frac{4(t^8+60t^6+134t^4+60t^2+1)^3}{(t-1)^8t^2(t+1)^8(t^2+1)^2}$
7	$\frac{(t^2-t+7)(t^2+t+7)(t^4+5t^2+1)^3}{t^2}$	$\frac{(t^2-t+7)(t^2+t+7)(t^4+245t^2+2401)^3}{t^{14}}$

注记. 在定理1和定理2的证明中，我们观察到，若 E 与 E' 是定义在 $\mathbb{Q}$上的两条椭圆曲线，且彼此3-同源或7-同源，则

$$\sqrt{\Delta(E)} \in \mathbb{Q} \quad \text{if and only if} \quad \sqrt{\Delta(E')} \in \mathbb{Q}.$$

本文最后一个主要结果聚焦于复乘的情形。该定理刻画了定义在 $\mathbb{Q}$上的、具有复乘且判别式为平方的椭圆曲线。特别是，该结果断言，不存在两条定义在$\mathbb{Q}$ 上的同源椭圆曲线，且它们都具有复乘和平方判别式。

定理3。 设 E 是定义在 $\mathbb{Q}$ 上的一条具有复乘的椭圆曲线。那么 $\sqrt{\Delta(E)} \in \mathbb{Q}$ 当且仅当 E 与某个 $t \in \mathbb{Q}^*$ 所对应的 E_{-t^2}： $y^2 = x^3 - t^2x$ 在 $\mathbb{Q}$上同构。特别地，若 E' 是定义在 $\mathbb{Q}$ 上的一条与 E 同源的椭圆曲线，那么 $\sqrt{\Delta(E')} \notin \mathbb{Q}$。

致谢。 本项目由 Arman Zargar 提出，因此我们感谢他提出最初的问题，这些问题启发了本研究。我们也感谢审稿人提出的许多详细意见，这些意见帮助我们改进了论文。

2. Twists、 isogenies and complex multiplication.

本节将介绍椭圆曲线理论中的一些基本概念，以便建立算术判据，用于判断椭圆

定义在 $\mathbb{Q}$ 上的曲线的判别式是否为平方（见命题 4）。本节最后，我们将给出定理 3 的证明。

2.1. 扭曲。 设 $E: y^2 = x^3 + Ax + B$ 是定义在 $\mathbb{Q}$上的椭圆曲线。我们分别用 $\Delta(E)$ 和 $j(E)$ 表示它的判别式和 j-不变量:

$$\Delta(E) = -16\left(4A^3 + 27B^2\right) \quad \text{and} \quad j(E) = -1728\frac{(4A)^3}{\Delta(E)}.$$

E 的 j-不变量是该曲线 $\mathbb{Q}$-同构类的不变量，且与所选取的具体方程无关（参见 [8, III 命题 1.4]）。此外，任何定义在$\mathbb{Q}$上且在 $\mathbb{Q}$ 上同构于 E 的椭圆曲线，都有如下形式的短魏尔斯特拉斯模型:

$$\begin{array}{lll} \text{(i)} & E^d : y^2 = x^3 + d^2Ax + d^3B & \text{if } j(E) \neq 0, 1728, \\ \text{(ii)} & E^d : y^2 = x^3 + dAx & \text{if } j(E) = 1728, \\ \text{(iii)} & E^d : y^2 = x^3 + dB & \text{if } j(E) = 0, \end{array}$$

其中 d 是 $\mathbb{Q}^*/(\mathbb{Q}^*)^{n(E)}$ 中的整数；若 $j(E) \neq 0, 1728$，则 $n(E) = 2$（分别为 4 或 6）（参见 [8, X §5]）。椭圆曲线 E^d 称为 E的 d-扭曲；在特殊情形 $j(E) \neq 0, 1728$ 下，它称为 E的 d-二次扭曲。注意，我们有

$$\Delta(E^d) = \begin{cases} d^6\Delta(E) & \text{if } j(E) \neq 0, 1728, \\ d^3\Delta(E) & \text{if } j(E) = 1728, \\ d^2\Delta(E) & \text{if } j(E) = 0. \end{cases}$$

以下结果在定理 1、2 和 3 的证明中起着关键作用。尽管它很基础且可能广为人知，但我未能在文献中找到确切的出处；因此，这里给出了它的证明。

命题 4. 设 E 是定义在 $\mathbb{Q}$ 上的椭圆曲线。那么 $\sqrt{\Delta(E)} \in \mathbb{Q}$ 当且仅当

- $j(E) = t^2 + 1728$，其中某个 $t \in \mathbb{Q}^*$ 满足该条件，或者
- $j(E) = 1728$，并且 E 与 $y^2 = x^3 - s^2x$ 在 $\mathbb{Q}$ 上同构，其中某个 $s \in \mathbb{Q}^*$ 满足该条件。

证明。 首先假设 $j_0 = j(E)$，其中 $j_0 \neq 0,1728$，并考虑椭圆曲线

$$E_{j_0} : y^2 = x^3 - 27\frac{j_0}{j_0 - 1728}x + 54\frac{j_0}{j_0 - 1728}.$$

直接计算可得

$$j(E_{j_0}) = j_0 \qquad \text{and} \qquad \Delta(E_{j_0}) = 2^{12} \cdot 3^{12}\frac{j_0^2}{(j_0 - 1728)^3}.$$

因此存在 $d \in \mathbb{Q}^*/(\mathbb{Q}^*)^2$，使得 E 与 $E_{j_0}^d$ $\mathbb{Q}$-同构。特别地,

$$\Delta(E) = \Delta(E_{j_0}^d) \equiv (j_0 - 1728) \bmod (\mathbb{Q}^*)^2.$$

因此，$\sqrt{\Delta(E)} \in \mathbb{Q}$ 当且仅当对某个 $t \in \mathbb{Q}$有 $j(E) = 1728 + t^2$。特别地，由于$j(E) \neq 1728$，故 $t \neq 0$。

现假设 $j(E) = 0$，并考虑满足 $j(E_0) = 0$与 $\Delta(E_0) = -3 \cdot 12^2$的椭圆曲线 E_0： $y^2 = x^3 + 1$。也就是说，对某个 $d \in \mathbb{Q}^*/(\mathbb{Q}^*)^6$， E 与 E_0^d $\mathbb{Q}$-同构。特别地

$$\Delta(E) = \Delta(E_0^d) \equiv -3 \bmod (\mathbb{Q}^*)^2.$$

这就证明了：若 $\sqrt{j(E)} = 0$，则 $\sqrt{\Delta(E)} \notin \mathbb{Q}$。

最后，假设 $j(E) = 1728$，并考虑满足 $j(E_{1728}) = 1728$ 且 $\Delta(E_{1728}) = -8^2$ 的椭圆曲线 E_{1728}： $y^2 = x^3 + x$。也就是说，对于某个 $d \in \mathbb{Q}^*/(\mathbb{Q}^*)^4$， E 与 E_{1728}^d 是 $\mathbb{Q}$-同构的。特别地

$$\Delta(E) = \Delta(E_{1728}^d) \equiv -d \bmod (\mathbb{Q}^*)^2.$$

因此，当且仅当存在某个 $s \in \mathbb{Q}^*$ 使得 $\sqrt{\Delta(E)} \in \mathbb{Q}$ 当且仅当 $-d = s^2$。 □

2.2. **定义在 $\mathbb{Q}$ 上的同源**。设 E 是定义在 $\mathbb{Q}$ 上的椭圆曲线，且 $N \in \mathbb{Z}$、$N > 1$。如果 E 具有一个（有理的）N-同源，即存在一个次数为 N 的（循环）同源 ϕ，使得对于任意 $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$，都有 ${}^{\sigma}\phi = \phi$，则称 E 具有一个（有理的）N-同源。等价地，E 具有一个定义在有理数域上的 N 阶（循环）子群。

有理同源的完整分类得益于 Fricke、Kenku、Klein、Kubert、Ligozat、Mazur 和 Ogg 等人的工作而完成（总结见 [5, 表1和 2]）：

定理 5。设 E 和 E' 是定义在 $\mathbb{Q}$ 上的两个 N-同源椭圆曲线。那么

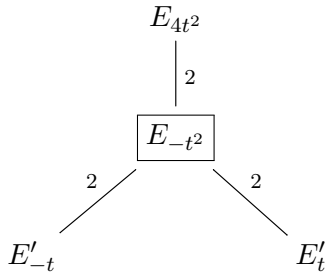
(i) $N \in \{2,3,4,5,6,7,8,9,10,12,13,16,18,25\}$。在此情形下，同构类有无穷多个，附录中的表 *4* 展示了 E 和 E' 的 j-不变量；或者(ii) $N \in \{11,14,15,17,19,21,27,37,43,67,163\}$。在此情形下，同构类只有有限多个，附录中的表 *5* 展示了 E 和 E' 的 j-不变量。

给定一个定义在 $\mathbb{Q}$ 上的椭圆曲线 $\mathbb{Q}$-同源类，其同源图由该同源类中每条椭圆曲线对应的一个顶点，以及该同源类中椭圆曲线之间每个有理素数次数同源对应的一条边组成，边上标注其次数。$\mathbb{Q}$ 上椭圆曲线的同源图最早见于所谓的安特卫普表 [1]。尽管首个证明（即将发表）似乎出自 Chiloyan 和 Lozano-Robledo [2, 定理 1.2]。

2.3. **在 $\mathbb{Q}$上的复乘**。众所周知，定义在 $\mathbb{Q}$ 上且具有复乘的椭圆曲线共有 13 个同构类（参见 [9, A §3]）。以下列表给出这十三个 j-不变量：

$$\mathcal{CM} = \left\{ \begin{array}{ccccccc} 0, & 2^4\cdot 3^3\cdot 5^3, & -2^{15}\cdot 3\cdot 5^3, & 2^6\cdot 3^3, & 2^3\cdot 3^3\cdot 11^3, & -3^3\cdot 5^3, & 3^3\cdot 5^3\cdot 17^3, \\ 2^6\cdot 5^3, & -2^{15}, & -2^{15}\cdot 3^3, & -2^{18}\cdot 3^3\cdot 5^3, & -2^{15}\cdot 3^3\cdot 5^3\cdot 11^3, & -2^{18}\cdot 3^3\cdot 5^3\cdot 23^3\cdot 29^3 & \end{array} \right\}.$$

定理 *3* 的证明。假设 $j(E) \in \mathcal{CM} \setminus \{1728\}$。那么，直接计算可得 $j_0 - 1728$ 不是平方。由命题 4 可知 $\sqrt{\Delta(E)} \notin \mathbb{Q}$。现在，若 $j(E) = 1728$，命题 4 表明 $\sqrt{\Delta(E)} \in \mathbb{Q}$ 当且仅当 E 与 E_{-t^2} 在 $\mathbb{Q}$ 上同构：$y^2 = x^3 - t^2x$ 对某个 $t \in \mathbb{Q}^*$ 成立。最后，与 E_{-t^2} 的 $\mathbb{Q}$- 同源类相关联的同源图为（参见 [2, 表5]）：



其中 E_{4t^2}：$y^2 = x^3 + 4t^2x$ 且 $E'_{\pm t}$：$y^2 = x^3 - 11t^2x \pm 14t^3$。注意，$j(E_{4t^2}) = 1728$ 且$j(E_{\pm t'}) = 2^3\cdot 3^3\cdot 11^3 \in \mathcal{CM}$。由于 $\Delta(E_{4t^2}) = -2^{12}t^6$ 和 $\Delta(E'_{\pm t}) = 2^9t^6$ 都不是完全平方数，故证明完成。

3. Proof of Theorem 1 and 2

具有复乘的性质在同源下保持不变。换句话说，如果 E 和 E' 是同源椭圆曲线，那么它们要么都具有复乘，要么都不具有复乘。复乘的情形已在定理3中讨论。因此，从现在起，我们假设所考虑的所有椭圆曲线都不具有复乘。在证明的其余部分，设 E 和 E' 是定义在 $\mathbb{Q}$上的两条 N-同源椭圆曲线，且都不具有复乘。特别地，N不属于 $\{14,19,27,43,67,163\}$（参见附录中的表 5）。

N	$F_N(h)$	$G_N(h)$
2	$h(h+64)$	$h+64$
3	h	h
4	$h(h+16)$	$h+16$
5	$h(h^2+22h+125)$	$h(h^2+22h+125)$
6	$h(h+8)$	$h+9$
7	h	h
8	h^2-16	h
9	h^3-27	h^3-27
10	$h(h-4)(h^2+4)$	$(h+1)(h^2+4)$
12	$(h^2-1)(h^2-9)$	$h(h-1)(h+3)$
13	$h(h^2+6h+13)$	$h(h^2+6h+13)$
16	$(h^2-4)(h^2+4)$	$h(h^2+4)$
18	$h(h^3-8)$	h^3+1
25	$(h-1)\left(h^2+4\right)\left(h^4+h^3+6h^2+6h+11\right)$	$(h-1)\left(h^2+4\right)\left(h^4+h^3+6h^2+6h+11\right)$

TABLE 1.

引理6. 设 E 是定义在 $\mathbb{Q}$上的椭圆曲线。若 E 存在一个 N-同源，其中 $N \in \{11, 15,17、21、37\}$，则 $\sqrt{\Delta(E)} \notin \mathbb{Q}$。

证明。令 J_N 表示有理数域 $\mathbb{Q}$ 上可承认 N-同源的椭圆曲线的 j-不变量集合。由定理 5 可知，这些集合是有限的，且列于附录中的表 5。令 $j_0 = j(E) \in J_N$。直接计算可得，$j_0 - 1728$ 不是平方。由命题 4 可知，$\sqrt{\Delta(E)} \notin \mathbb{Q}$。□

令 $N \in \{2,3,4,5,6,7,8,9,10,12,13,16,18,25\}$，并令 E，E' 为定义在 $\mathbb{Q}$上的 N-同源椭圆曲线。则存在 $h \in \mathbb{Q}$ 使得 $j(E) = j_N(h)$ 且 $j(E') = j'_N(h)$（参见附录中的表 4）。

设 $F_N(h)$ $G_N(h) \in \mathbb{Q}[h]$ 为表1中所定义的多项式。于是我们有

$$F_N(h) \equiv (j_N(h) - 1728) \bmod (\mathbb{Q}[h])^2 \qquad \text{and} \qquad G_N(h) \equiv (j'_N(h) - 1728) \bmod (\mathbb{Q}[h])^2.$$

我们定义曲线

$$C_N : y^2 = F_N(h) \quad \text{and} \quad X_N : \left\{(h, y, z) \,:\, y^2 = F_N(h), z^2 = G_N(h)\right\},$$

以及集合

$$C_N^*(\mathbb{Q}) := \{h \,:\, (h, y) \in C_N(\mathbb{Q}) \text{ and } j_N(h) \neq \infty\},$$
$$X_N^*(\mathbb{Q}) := \{h \,:\, (h, y, z) \in X_N(\mathbb{Q}) \text{ and } j_N(h), j'_N(h) \neq \infty\}.$$

根据命题 4，曲线 C_N 参数化了容许 N-同源且具有平方判别式的椭圆曲线，而曲线 X_N 参数化了具有平方判别式的 N-同源椭圆曲线对。特别地：

- 存在定义在 $\mathbb{Q}$ 上的椭圆曲线 E，它容许一个满足 $\sqrt{\Delta(E)} \in \mathbb{Q}$ 的 N-同源，当且仅当 $C_N^*(\mathbb{Q}) \neq \emptyset$。
- 存在两条在 $\mathbb{Q}$ 上定义的 N-同源椭圆曲线 E 和 E'，使得 $\sqrt{\Delta(E)}, \sqrt{\Delta(E')} \in \mathbb{Q}$ 当且仅当 $X_N^*(\mathbb{Q}) \neq \emptyset$。

注。 基于 Rouse–Zureick-Brown [7]和 Zywina [10], 的结果，Morrow [6]构造了复合层模曲线的模型，其有理点参数化了在 $\mathbb{Q}$ 上具有同时非满复合伽罗瓦像的椭圆曲线。他的工作中得到的一些曲线最终被证明等价于本文中的一些曲线，尽管它们在此处出现于完全不同的背景下。

定理 1 的证明。首先，我们注意到本研究仅限于值集$N \in \{2,3,4,5,6,7,8,9,10,12,13,16,18,25\}$。表2提供了有关每个指定 N对应的曲线 C_N 的重要信息。

N	$g(C_N)$	h	有理点	LMFDB
2	0	$16\frac{t^2}{t+1}$		
3	0	t^2		
4	0	$4\frac{t^2}{t+1}$		
5	1	–	$C_5(\mathbb{Q}) = \{(0,\ 0)\}$	20.a2
6	0	$2\frac{t^2}{t+1}$		
7	0	t^2		
8	0	$2\frac{t^2+2t+2}{t+1}$		
9	1	–	$C_9(\mathbb{Q}) = \{(3,0)\}$	36.a3
10	1	–	$C_{10}(\mathbb{Q}) = \{(4,\ 0),\ (0,\ 0),\ (-1,\ \pm 5)\}$	20.a4
12	1	–	$C_{12}(\mathbb{Q}) = \{(0,\pm 3),(\pm 3,0),(\pm 1,0)\}$	24.a4
13	1	–	$C_{13}(\mathbb{Q}) = \{(0,\ 0)\}$	52.a2
16	1	–	$C_{16}(\mathbb{Q}) = \{(\pm 2,0)\}$	32.a4
18	1	–	$C_{18}(\mathbb{Q}) = \{(0,\ 0),\ (2,\ 0),\ (-1,\ \pm 3)\}$	36.a4
25	3	–	$C_{25}(\mathbb{Q}) = \{(1,0)\}$	

TABLE 2. 曲线 C_N 的数据

表2说明：对于第一列集合 $\{2,3,4,5,6,7,8,9,10,12,13,16,18,25\}$ 中的每个整数 N，第二列列出曲线 C_N 的亏格。第三列给出 h 的参数化，该参数化由 ϕ_N 得到（当亏格为 0 时）；否则标记为“–”。第四列显示亏格大于 0 时 C_N 的集合 $C_N(\mathbb{Q})$。最后一列给出当 C_N 为椭圆曲线时对应的 LMFDB 标签。

亏格为(C_N) 的情形 $= 0$。曲线 C_N： $y^2 = F_N(h)$ 在 $N \in \{2,3,4,6,7,8\}$ 时亏格为 0。由于对于 $N \in \{2,3,4,6,7\}$，$(0,\ 0) \in C_N(\mathbb{Q})$，且 $(4,\ 0) \in C_8(\mathbb{Q})$，我们可以计算参数化$\phi_N$： $\mathbb{A}^1(\mathbb{Q}) \longrightarrow C_N(\mathbb{Q})$。

例如，对于 $N = 2$，我们有 C_2： $y^2 = h(h+64)$ 和 $\phi_2(t) = \left(\frac{16t^2}{t+1}, \frac{16t}{}\left(\frac{t+2}{t+1}\right)\right)$。因此

$$C_2^*(\mathbb{Q}) = \left\{\frac{16t^2}{t+1} \ : \ t \in \mathbb{Q}\right\}.$$

N 的情形 $\in \{3,4,6,7,8\}$ 类似，完整信息见表2 .

亏格的情形(C_N) $= 1$。曲线 C_N: $y^2 = F_N(h)$ 在 $N \in \{5, 9, 10, 12, 13, 16, 18\}$ 时亏格为 1。我们的目标是计算 C_N 上的仿射 $\mathbb{Q}$-有理点，以证明它们对应于映射 $j_N(h)$ 的尖点。

例如，考虑 $N = 5$ 的情形。参数化具有平方判别式且存在 5-同源的椭圆曲线的曲线由下式给出：

$$C_5 \colon y^2 = h(h^2 + 22h + 125).$$

这是一条定义在 $\mathbb{Q}$ 上的椭圆曲线，其点 $(0,0) \in C_5(\mathbb{Q})$。它的 LMFDB 标签是 20.a2（参见 [4]）。这条椭圆曲线的莫德尔–韦伊群同构于 $\mathbb{Z}/2\mathbb{Z}$，这表明$C_5(\mathbb{Q}) = \{(0,0)\}$。

因此，我们已经证明，如果 E 是一条在 $\mathbb{Q}$ 上存在 5-同源的椭圆曲线，那么$\sqrt{\Delta(E)} \notin \mathbb{Q}$。

$N \in \{9, 10, 12, 13, 16, 18\}$ 的情形类似，完整信息见表2。

亏格情形(C_N) > 1。只有一条亏格大于 1 的曲线 C_N，即 C_{25}。我们可以断言 $C_{25}(\mathbb{Q}) = \{(1,0)\}$，且 $C_{25}^*(\mathbb{Q}) = \emptyset$，因为我们上文已经证明，如果 E 是一条在 $\mathbb{Q}$ 上存在 5-同源的椭圆曲线，那么 $\sqrt{\Delta(E)} \notin \mathbb{Q}$。这是因为，如果 E 存在 25-同源，那么它必然存在 5-同源。

定理 2 的证明。首先，注意到由定理 1 可知，只需研究 N 属于集合 $N \in \{2, 3, 4, 6, 7, 8\}$ 的情形。表 3 提供了关于每个指定 N 对应曲线 X_N 的重要信息。值得注意的是， X_N 的亏格满足 genus(X_N) ≤ 1。

亏格为(X_N) $= 0$ 的情形。此情形类似于曲线 C_N 的亏格为 0 的情形。当 $N \in \{2, 3, 4, 7\}$ 时，曲线 X_N 的亏格为 0。由于对于 $N \in \{3, 7\}$，(0<style id="8">，0<style id="10">，0) $\in X_N(\mathbb{Q})$，(0<style id="15">，0<style id="17">，8) $\in X_2(\mathbb{Q})$，且 (0<style id="21">，0<style id="23">，4) $\in X_4(\mathbb{Q})$，我们可以计算一个参数化

$$\psi_N \colon \mathbb{A}^1(\mathbb{Q}) \longrightarrow X_N(\mathbb{Q}).$$

例如，对于 $N = 2$，我们有

$$X_2 : \{(h, y, z) \, : \, y^2 = h(h + 64), \quad z^2 = h + 64\},$$

以及参数化

$$\psi_2(t) = \left(\left(4\frac{t^2 - 1}{t} \right)^2 , 16\frac{t^4 - 1}{t^2}, 4\frac{t^2 + 1}{t} \right).$$

因此，

$$X_2^*(\mathbb{Q}) = \left\{ \left(4\frac{t^2 - 1}{t} \right)^2 \, : \, t \in \mathbb{Q} \right\}.$$

$N \in \{3, 4, 7\}$ 的情形类似，完整细节见表 3。

亏格为(X_N) $= 1$的情形。此情形类似于曲线 C_N 的亏格为 1 的情形。当 $N \in \{6, 8\}$ 时，曲线 X_N 的亏格为 1。我们的目标是计算 X_N 上的仿射 $\mathbb{Q}$-有理点，以证明它们对应于映射 $j_N(h)$ 或 $j'_N(h)$ 的尖点。

让我们详细分析 $N = 6$ 的情形。曲线 X_6 是定义在 $\mathbb{Q}$ 上的椭圆曲线，因为它是一条亏格为 1 且包含有理点 $(0,\ 0,\ 3) \in X_6(\mathbb{Q})$ 的曲线。其 LMFDB 标签为 24.a4。这条椭圆曲线的 Mordell–Weil 群同构于 $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$。因此，我们有

$$X_6(\mathbb{Q}) = \{(-9, \pm 3, 0), (-8, 0, \pm 1), (0, 0, \pm 3)\}.$$

因此，我们已经证明，如果 E 和 E' 构成一对定义在 $\mathbb{Q}$上的 6-同源椭圆曲线，那么$\sqrt{\Delta(E)}\ \sqrt{\Delta(E')} \notin \mathbb{Q}$。

情形 $N = 8$ 与之类似，完整细节见 表 3。

N	$g(X_N)$	h	有理点	LMFDB
2	0	$\left(4\frac{t^2-1}{t}\right)^2$		
3	0	t^2		
4	0	$\left(2\frac{t^2-1}{t}\right)^2$		
6	1	–	$X_6(\mathbb{Q}) = \{(-9,\pm 3,0),(-8,0,\pm 1),(0,0,\pm 3)\}$	24.a4
7	0	t^2		
8	1	–	$X_8(\mathbb{Q}) = \{(4,0,\pm 2)\}$	32.a4

TABLE 3. 曲线 X_N 的数据

表 3 说明：本表与表2类似。对于第一列集合 $\{2,3,4,6,7,8\}$中的每个整数 N，第二列列出曲线 X_N的亏格。第三列给出在亏格为0的情形下由 ψ_N 得到的 h的参数化；否则标记为“–”。第四列在 X_N 的亏格大于0的情形下列出集合 $X_N(\mathbb{Q})$。最后一列在 X_N 为椭圆曲线时给出相应的 LMFDB 标签。

APPENDIX: j-INVARIANTS SUCH THAT E AND E' ARE N-ISOGENOUS

为求完整起见，我们在本附录中列出定义在 $\mathbb{Q}$ 上的同源椭圆曲线对的 j-不变量。这些表格主要摘自 [5]。表 4 展示了模曲线 $X_0(N)$ 亏格为 0 时的 j-映射，其余情形列于表 5。

REFERENCES

[1] B.J. Birch、W. Kuyk（编），*Modular Functions of One Variable IV*。《数学讲义》第 476 卷，施普林格出版社，1975 年。[2] G. Chiloyan，´A. Lozano-Robledo，*A classification of isogeny-torsion graphs of $\mathbb{Q}$-isogeny classes of elliptic curves*。《伦敦数学会会刊》**8**（2021），1–34。[3] I. Garc´ıa-Selfa、E. Gonzalez-Jimenez、J.M. Tornero，*Galois theory discriminants and torsion subgroup of elliptic curves* **214** 2010 8, 1340 1346。《纯粹与应用代数杂志》（），第 – 期。[4] LMFDB 协作组。*The L-functions and modular forms database*。https://www.lmfdb.org，2025 年。[在线；访问日期： 2025] 年 8 月 24 日。[5] ´A. Lozano-Robledo，*On the field of definition of p-torsion points on elliptic curves over the rationals*。《数学年刊》**357**（2013），279–305。[6] J.S. Morrow，*Composite images of Galois for elliptic curves over $\mathbb{Q}$ and entanglement fields.* 。《数学计算》**88**（2019），2389–2421。[7] J. Rouse 和 D. Zureick-Brown，*Elliptic curves over $\mathbb{Q}$ and 2-adic images of Galois.* 。《数论研究》**1**（2015），论文编号 12。[8] J. H. Silverman，*The Arithmetic of Elliptic Curves*，《数学研究生教材》第 106 卷。施普林格出版社，Dordrecht，2009 年。[9] J. H. Silverman，*Advanced Topics in the Arithmetic of Elliptic Curves*，《数学研究生教材》第 151 卷。施普林格出版社，纽约，1994 年。[10] D. Zywina，*On the possible images of the mod ℓ representations associated to elliptic curves over $\mathbb{Q}$*。arXiv:1508.07660。

DEPARTAMENTO DE MATEMÁTICAS, UNIVERSIDAD AUTÓNOMA DE MADRID,MADRID, SPAIN,
Email address: enrique.gonzalez.jimenez@uam.es*URL*:
http://www.uam.es/enrique.gonzalez.jimenez

N	$j_N = j(E)$	$j'_N = j(E')$
2	$j_2(h) = \frac{(h+16)^3}{h}$	$j'_2(h) = \frac{(h+256)^3}{h^2}$
3	$j_3(h) = \frac{(h+27)(h+3)^3}{h}$	$j'_3(h) = \frac{(h+27)(h+243)^3}{h^3}$
4	$j_4(h) = \frac{(h^2+16h+16)^3}{h(h+16)}$	$j'_4(h) = \frac{(h^2+256h+4096)^3}{h^4(h+16)}$
5	$j_5(h) = \frac{(h^2+10h+5)^3}{h}$	$j'_5(h) = \frac{(h^2+250h+5^5)^3}{h^5}$
6	$j_6(h) = \frac{(h+6)^3(h^3+18h^2+84h+24)^3}{h(h+8)^3(h+9)^2}$	$j'_6(h) = \frac{(h+12)^3(h^3+252h^2+3888h+15552)^3}{h^6(h+8)^2(h+9)^3}$
7	$j_7(h) = \frac{(h^2+13h+49)(h^2+5h+1)^3}{h}$	$j'_7(h) = \frac{(h^2+13h+49)(h^2+245h+2401)^3}{h^7}$
8	$j_8(h) = \frac{(h^4-16h^2+16)^3}{(h^2-16)h^2}$	$j'_8(h) = \frac{(h^4+240h^3+2144h^2+3840h+256)^3}{(h-4)^8h(h+4)^2}$
9	$j_9(h) = \frac{h^3(h^3-24)^3}{h^3-27}$	$j'_9(h) = \frac{(h+6)^3(h^3+234h^2+756h+2160)^3}{(h-3)^8(h^3-27)}$
10	$j_{10}(h) = \frac{(h^6-4h^5+16h+16)^3}{(h+1)^2(h-4)h^5}$	$j'_{10}(h) = \frac{(h^6+236h^5+1440h^4+1920h^3+3840h^2+256h+256)^3}{(h-4)^{10}h^2(h+1)^5}$
12	$j_{12}(h) = \frac{(h^2-3)^3(h^6-9h^4+3h^2-3)^3}{h^4(h^2-9)(h^2-1)^3}$	
	$j'_{12}(h) = \frac{(h^2+6h-3)^3(h^6+234h^5+747h^4+540h^3-729h^2-486h-243)^3}{(h-3)^{12}(h-1)^3h^4(h+1)^3(h+3)^3}$	
13	$j_{13}(h) = \frac{(h^2+5h+13)(h^4+7h^3+20h^2+19h+1)^3}{h}$	
	$j'_{13}(h) = \frac{(h^2+5h+13)(h^4+247h^3+3380h^2+15379h+28561)^3}{h^{13}}$	
16	$j_{16}(h) = \frac{(h^8-16h^4+16)^3}{h^4(h^4-16)}$	
	$j'_{16}(h) = \frac{(h^8+240h^7+2160h^6+6720h^5+17504h^4+26880h^3+34560h^2+15360h+256)^3}{(h-2)^{16}h(h+2)^4(h^2+4)}$	
18	$j_{18}(h) = \frac{(h^3-2)^3(h^9-6h^6-12h^3-8)^3}{h^9(h^3-8)^3(h+1)^2}$	
	$j'_{18}(h) = \frac{(h^3+6h^2+4)^3(h^9+234h^8+756h^7+2172h^6+1872h^5+3024h^4+48h^3+3744h^2+64)^3}{(h-2)^{18}h^9(h+1)^2(h^2-h+1)^2(h+2h+4)^2}$	
25	$j_{25}(h) = \frac{(h^{10}+10h^8+35h^6-12h^5+50h^4-60h^3+25h^2-60h+16)^3}{h^5+5h^3+5h-11}$	
	$j'_{25}(h) = \frac{(h^{10}+240h^9+2170h^8+8880h^7+34835h^6+83748h^5+206210h^4+313380h^3+503545h^2+424740h+375376)^3}{(h-1)^{25}(h^4+h^3+6h^2+6h+11)}$	

TABLE 4. j不变量，使得 E 和 E' 是 N-同源

N	$j_N = j(E)$	$j'_N = j(E')$	CM?
11	$-11 \cdot 131^3$	-11^2	no
	-2^{15}	-2^{15}	yes
14	$-3^3 \cdot 5^3$	$3^3 \cdot 5^3 \cdot 17^3$	yes
15	$-5^2/2$	$5 \cdot 211^3/2^{15}$	no
	$-5^2 \cdot 241^3/2^3$	$-5 \cdot 29^3/2^5$	no
17	$-17^2 \cdot 101^3/2$	$-17 \cdot 373^3/2^{17}$	no
19	$-2^{15} \cdot 3^3$	$-2^{15} \cdot 3^3$	yes
21	$-3^2 \cdot 5^6/2^3$	$-3^3 \cdot 5^3 \cdot 383^3/2^7$	no
	$3^3 \cdot 5^3/2$	$-3^2 \cdot 5^3 \cdot 101^3/2^{21}$	no
27	$-2^{15} \cdot 3 \cdot 5^3$	$-2^{15} \cdot 3 \cdot 5^3$	yes
37	$-7 \cdot 11^3$	$-7 \cdot 137^3 \cdot 2083^3$	no
43	$-2^{18} \cdot 3^3 \cdot 5^3$	$-2^{18} \cdot 3^3 \cdot 5^3$	yes
67	$-2^{15} \cdot 3^3 \cdot 5^3 \cdot 11^3$	$-2^{15} \cdot 3^3 \cdot 5^3 \cdot 11^3$	yes
163	$-2^{18} \cdot 3^3 \cdot 5^3 \cdot 23^3 \cdot 29^3$	$-2^{18} \cdot 3^3 \cdot 5^3 \cdot 23^3 \cdot 29^3$	yes

TABLE 5. j-不变量，使得 E 与 E' 是 N-同源