arXiv:2602.01380v1 [math.NT] 1 Feb 2026

某些非本原四次数域上的等差数列中的平方数

ENRIQUE GONZ´ALEZ–JIM´ENEZ 和 NGUYEN XUAN THO

摘要。设 D 为无平方因子整数。在满足关于 D的某些条件时，我们刻画了 $\mathbb{Q}(\sqrt{D})$的二次扩张上的非恒定平方数等差数列。

1. 引言

费马于1640年指出，在 $\mathbb{Q}$上不存在由四个平方数组成的非恒定等差数列，欧拉于1780年证明了这一点。自然会想到，在数域上会出现什么情况。在二次域上，Xarles [14]证明不存在由六个平方数组成的非恒定等差数列；Gonz´alez-Jim´enez 和 Xarles [9]刻画了由五个平方数组成的非恒定等差数列。在三次域上，Bremner 和 Siksek [3] 证明不存在由五个平方数组成的非恒定等差数列。

本文将 Xarles [14] 以及 Gonz´ález-Jim´enez 和 Xarles [9] 的结果推广到 $\mathbb{Q}(\sqrt{D})$ 的二次扩张，其中 D 是满足椭圆曲线的 D-二次扭曲条件的无平方因子整数

$$E_0 : y^2 = x^3 - x^2 - 9x + 9 \qquad \text{and} \qquad E_1 : y^2 = x^3 - x^2 + x.$$

对于任意椭圆曲线 E 和整数 D，我们将 E的 D-二次扭曲记为 E^D 。

设 n为正整数， K为一个域。设 $a_1, \ldots, a_n \in K$，使得 $(a_1^2, a_2^2, \ldots, a_n^2)$ 是一个长度为 n 的等差数列。对于任意 $s \in K^*$，我们称该等差数列与 $(s^2a_1^2, s^2a_2^2, \ldots, s^2a_n^2)$ 等价，也称其与等差数列 $(a_n^2, \ldots, a_2^2, a_1^2)$ 等价。如果 $a_1, \ldots, a_n \in K$ 且对于 K的任意真子域 F， $\{a_1, \ldots, a_n\} \not\subset F$，则称 $(a_1^2, a_2^2, \ldots, a_n^2)$ 在数域 K 上恰当定义。令 $\overline{i} = \sqrt{-1}$。

本文的主要定理如下。

定理1. 设 D 为无平方因子整数， $D \neq -1$、 ± 2、 3，满足 秩$_{\mathbb{Z}}\, E_1^{\pm D}(\mathbb{Q}) = 0$，且 K 是 $\mathbb{Q}(\sqrt{D})$ 的二次扩张。那么

(A) 若 秩$_{\mathbb{Z}}\, E_0^D(\mathbb{Q}) = 0$，则不存在任何在 K 上恰当定义的五个平方的非恒定等差数列。(B) 若 秩$_{\mathbb{Z}}\, E_0^D(\mathbb{Q}) \neq 0$，且 $\mathbb{Q}(\sqrt{D})$ 的类数为 1，则在 K 上恰当定义的五个平方的非恒定等差数列，在等价意义下具有如下形式：$\big(a^2$、 b^2、 c^2、 $\alpha\, d^2$、 $e^2\big)$，其中 a、 b、 c、 d、 e、 $\alpha \in \mathbb{Q}(\sqrt{D})$ ，且 α 为非平方数。

定理 2。 存在一个在二次扩张 K 上恰当定义的五个平方数的非恒定等差数列

- $\mathbb{Q}(i)$ 当且仅当 $K = \mathbb{Q}(i, \sqrt{2})$。在这种情况下，$(-2, -1, 0, 1, 2)$ 是定义在 K上的五个平方数的非恒定等差数列，且在等价意义下唯一。
- $\mathbb{Q}(\sqrt{3})$ 当且仅当 $K = \mathbb{Q}(\sqrt{3}, \sqrt{2})$。在这种情况下，$(0,\ 1,\ 2,\ 3,\ 4)$ 是恰当定义在 K上的唯一一个（在等价意义下）非恒定五个平方数的等差数列。

日期：2026年2月3日。2020 数学主题分类。主要分类：11B25、11G05；次要分类：14G05。关键词和短语。平方数等差数列、二次扩张、椭圆曲线、有理点。第一作者获得由 MCIN/AEI/10.13039/501100011033 资助的 PID2022-138916NB-I00 项目，并获得欧洲区域发展基金“建设欧洲之路”的资助。第二作者获得越南国家科学技术发展基金会（NAFOSTED）资助（项目编号 101.04-2023.21）。

- $\mathbb{Q}(\sqrt{2})$ 当且仅当 $K=\mathbb{Q}(\sqrt{2},\sqrt{3})$、$K=\mathbb{Q}(\sqrt{2},i)$ 或 $K=\mathbb{Q}(\sqrt{2},\sqrt{\alpha})$ 成立，其中某个$\alpha\in\mathbb{Q}(\sqrt{2})$无平方因子。第一种情况下，$(0,1,2,3,4)$ 是恰当定义在 $\mathbb{Q}(\sqrt{2},\sqrt{3})$ 上的唯一一个（在等价意义下）非恒定五个平方数的等差数列；第二种情况下，$(-2,-1,0,1,2)$ 是恰当定义在 $\mathbb{Q}(\sqrt{2},i)$ 上的唯一一个（在等价意义下）非恒定五个平方数的等差数列。最后一种情况下，恰当定义在 K 上的非恒定五个平方数的等差数列，在等价意义下具有如下形式：$\left(a^2,b^2,c^2,\alpha\,d^2,e^2\right)$，其中 $a,b,c,d,e\in\mathbb{Q}(\sqrt{2})$。
- $\mathbb{Q}(\sqrt{-2})$ 当且仅当 $K=\mathbb{Q}(\sqrt{-2},i)$ 或 $K=\mathbb{Q}(\sqrt{-2},\sqrt{\alpha})$，其中 $\alpha\in\mathbb{Q}(\sqrt{-2})$ 是某个无平方因子的。在第一种情况下，$(-2,-1,0,1,2)$ 是在 $\mathbb{Q}(\sqrt{-2},i)$ 上恰当定义的五个平方的非常数等差数列，且在等价意义下唯一。在第二种情况下，在 K 上恰当定义的五个平方的非常数等差数列，在等价意义下具有如下形式：$\left(a^2,b^2,c^2,\alpha\,d^2,e^2\right)$，其中 $a,b,c,d,e\in\mathbb{Q}(\sqrt{-2})$。

注记。注意，若 $D\in\{-1,\pm2,3\}$，则 $\operatorname{rank}_{\mathbb{Z}}E_1^{\pm D}(\mathbb{Q})=0$ 且 $\operatorname{rank}_{\mathbb{Z}}E_0^{D}(\mathbb{Q})=0$。

定理3. 设 D 为无平方因子整数，使得

$$\operatorname{rank}_{\mathbb{Z}}E_1^{\pm D}(\mathbb{Q})=0\,,$$

且秩$_{\mathbb{Z}}E_0^{D}(\mathbb{Q})=0$，或者若秩$_{\mathbb{Z}}E_0^{D}(\mathbb{Q})\neq0$，则 $\mathbb{Q}(\sqrt{D})$ 的类数为1。则在 $\mathbb{Q}(\sqrt{D})$的任何二次扩张上，不存在任何恰当定义的六个平方数的非恒定等差数列。

注. 下列列表给出了所有满足秩$_{\mathbb{Z}}E_1^{\pm D}(\mathbb{Q})=$0且秩$_{\mathbb{Z}}E_0^{D}(\mathbb{Q})=0$的无平方因子整数 D、$|D|<200$:

$$-158,-123,-62,-51,-3,-2,-1,2,3,7,31,51,62,79,103,110,123,127,151,158,194,195,199.$$

若我们允许秩$_{\mathbb{Z}}E_0^{D}(\mathbb{Q})\neq0$且 $\mathbb{Q}(\sqrt{D})$的类数为1，则 $D\in\{-7,38,86\}$。

注。存在无平方因子整数 D，以及恰当定义在有理数域 $\mathbb{Q}(\sqrt{D})$ 的二次扩张上的非恒定六个平方数等差数列。例如，当 $D=409$ 时，

$$(7^2,13^2,17^2,(\sqrt{409})^2,23^2,(\sqrt{649})^2)$$

是恰当定义在 $\mathbb{Q}(\sqrt{409},\ \sqrt{649})$ 上的等差数列。

猜想 4。存在无穷多个五个平方数的非恒定等差数列，它们恰当定义在有理数域 $\mathbb{Q}(\sqrt{-2})$ 的二次扩张 K_1（分别为有理数域 $\mathbb{Q}(\sqrt{2})$ 的二次扩张 K_2）。

(i) 在 $\mathbb{Q}(\sqrt{-2})$ 的情形下，它们在等价意义下均具有如下形式：$\left(a^2,b^2,-2c^2,-md^2,-2e^2\right)$，其中 $a,b,c,d,e,m\in\mathbb{Z}$，且 $m>0$ 是无平方因子的。特别地，$K_1=\mathbb{Q}(\sqrt{-2},\sqrt{-m})$。(ii) 在 $\mathbb{Q}(\sqrt{2})$ 的情形下，它们在等价意义下均具有如下形式：$\left(2a^2,b^2,2c^2,m,e^2\right)$，其中 $a,b,c,e,m\in\mathbb{Z}$，且 m 是无平方因子的。特别地，$K_2=\mathbb{Q}(\sqrt{2},\sqrt{m})$。

猜想 4 得到了第 9 节中计算结果的支持。对于 $D\in\{-7,38,86\}$ 这些情形，并没有类似的猜想。

我们的方法不同于 [9] 和 [14]中的方法。我们采用 Mordell 在其论文 [11], 中的方法；他针对 Aigner [1] 和 Faddeev [4] 关于在二次域和三次数域中求解方程 $x^4+y^4=1$ 的结果，给出了另一种证明。Mordell 的方法优点在于计算十分具体。

另一个重要组成部分是关于椭圆曲线在基变换下挠子群增长的理论。假设秩$_{\mathbb{Z}}E_1^{\pm D}(\mathbb{Q})=0$, 那么确定某些定义在 $\mathbb{Q}$ 上的椭圆曲线在任意二次域上的挠子群就至关重要。这个问题的答案可在 LMFDB 在线数据库 [13] 中找到。近年来，挠点增长理论受到了广泛研究。特别值得一提的参考文献有[5, 6] 和 [7, 8, 12] （针对二次域）。

在以下小节中，我们列出与本文相关的所有椭圆曲线，以及关于二次域上有理点的必要信息。这些内容将在前述定理的证明中使用。

若干椭圆曲线的数据。表1展示了本文使用的椭圆曲线。对于每条曲线C_k，当 $k = 0$，1，……，6 时，第三列给出其在 LMFDB 数据库中的对应标签[13]，，第四列则列出与之 $\mathbb{Q}$同构的椭圆曲线。

表1：曲线

C_0	$y^2 = x^4 - 2x^3 + 2x^2 + 2x + 1$	192.a2	E_0
C_1	$y^2 = (x + 4)(x^2 + 4x + 16)$	24.a5	E_1
C_2	$y^2 = x(x^2 + 4x + 16)$	48.a5	E_1^{-1}
C_3	$y^2 = x(x + 4)(x^2 + 4x + 16)$	24.a5	E_1
C_4	$y^2 = x(x^2 + 14x + 1)$	24.a2	E_4
C_5	$y^2 = x^4 + 4x^2 + 16$	48.a4	E_6^{-1}
C_6	$y^2 = x^4 + 14x^2 + 1$	24.a4	E_6

注意，椭圆曲线 E_1，E_4 与 E_6 属于同一个 $\mathbb{Q}$-同源类。特别地，对任意整数 D，任意 D-二次扭转的秩都相同。特别地，对 $k = 1$，……，6，我们有秩$_{\mathbb{Z}}\, C_k(\mathbb{Q}) = 0$。设 E是定义在 $\mathbb{Q}$上的一条椭圆曲线。利用已知公式（见 [10]）

$$\mathrm{rank}_{\mathbb{Z}}\, E(\mathbb{Q}(\sqrt{D})) = \mathrm{rank}_{\mathbb{Z}}\, E(\mathbb{Q}) + \mathrm{rank}_{\mathbb{Z}}\, E^D(\mathbb{Q}),$$

我们得到，对 $k = 1$，……，6，秩$_{\mathbb{Z}}\, E_1^{\pm D}(\mathbb{Q}) = 0$等价于秩$_{\mathbb{Z}}\, C_k(\mathbb{Q}(\sqrt{D})) = 0$。假设对无平方因子整数 D有秩$_{\mathbb{Z}}\, E_1^{\pm D}(\mathbb{Q}) = 0$，则为了对 $k = 1$，……，6计算 $C_k(\mathbb{Q}(\sqrt{D}))$，我们需要计算 $\mathbb{Q}(\sqrt{D})$上的挠子群。在我们的特殊情形中，给定定义在 $\mathbb{Q}$上的椭圆曲线 E，仅有有限多个无平方因子整数 D 使得 $E(\mathbb{Q})_{\mathrm{tors}} \neq E(\mathbb{Q}(\sqrt{D}))_{\mathrm{tors}}$。若 E 的导子小于400000，这些无平方因子整数出现在LMFDB数据库 [13] 中，并列入表2。

表2：二次域上的挠点增长

E	D 使得 $E(\mathbb{Q})_{\mathrm{tors}} \neq E(\mathbb{Q}(\sqrt{D}))_{\mathrm{tors}}$
E_0	-2
E_1	$-1, \pm 3$
E_1^{-1}	$-1, \pm 3$
E_4	2,3,6
E_6	$\emptyset$
E_6^{-1}	$-1, \pm 3$

注意，对于这些椭圆曲线及 D 的取值，除 E_4^6 的情形外，我们有 $\mathrm{rank}_{\mathbb{Z}}\, E^D(\mathbb{Q}) = 0$。最后，对于任意无平方因子整数 D，表3和表4给出了 $C_k(\mathbb{Q}(\sqrt{D}))$，其中 $k = 1, \ldots, 6$。当$D = -1, 2, \pm 3$时，第二列中的点对应于 $C_k(\mathbb{Q})$，因此必须将它们加入相应的集合 $C_k(\mathbb{Q}(\sqrt{D}))$。

表 3. $C_k(\mathbb{Q}(\sqrt{D}))$ 对于 $k = 1,2,3,5,6$。

	$D \neq -1, \pm 3$	$D = -1$	$D = -3$	$D = 3$
C_1	$(-4,\ 0)$ $(0, \pm 8)$	$(-4 \pm 4i,\ \pm 8)$	$(-8,\ \pm 8\sqrt{-3})$ $(-2 \pm 2\sqrt{-3},\ 0)$	$(4 - 4\sqrt{3},\ \pm(24 - 16\sqrt{3}))$ $(4 + 4\sqrt{3},\ \pm(24 + 16\sqrt{3}))$
C_2	$(0,$ $0)$	$(\pm 4i,\ \pm 8i)$ $(-4,\ \pm 8i)$	$(-2 \pm 2\sqrt{-3},\ 0)$	$(4,\ \pm 8\sqrt{3})$
C_3	$(0,\ 0)$ $(-4,\ 0)$	$(-2 \pm 2i,\ \pm 8i)$	$(-2 \pm 2\sqrt{-3},\ 0)$ $(-2,\ \pm 4\sqrt{-3})$	$(-2 \pm 2\sqrt{3},\ \pm 8\sqrt{3})$
C_5	$(0, \pm 4)$	$(\pm 2i,\ \pm 4)$	$(\pm 1 \pm \sqrt{-3},\ 0)$	$(\pm 2,\ \pm 4\sqrt{3})$
C_6	$(0, \pm 1)$ $(\pm 1,\ \pm 4)$	–	–	–

表 4. $C_4(\mathbb{Q}(\sqrt{D}))$

	$D \neq 2,3,6$	$D = 3$	$D = 2$
C_4	$(0,\ 0)$ $(1,\ \pm 4)$	$(-1,\ -2\sqrt{3})$ $(7 \pm 4\sqrt{3},\ 0)$	$(-3 - 2\sqrt{2},\ \pm(8 + 6\sqrt{2}))$ $(-3 + 2\sqrt{2},\ \pm(8 - 6\sqrt{2}))$

引理 5. 设 D 为无平方因子整数，使得秩$_{\mathbb{Z}}\, E_0^D(\mathbb{Q}) = 0$。则 $E_0(\mathbb{Q}(\sqrt{D})) = E_0(\mathbb{Q})$，除非 $D = \pm 2$。

证明。表2表明，只有当 $D = -2$ 时，挠子群才会增大。因此，对于 $D \neq -2$，我们有 $E_0(\mathbb{Q}(\sqrt{D}))_{\text{tors}} = E_0(\mathbb{Q})_{\text{tors}}$。因此，若 $D \neq -2$ 且 $\text{rank}_{\mathbb{Z}}\, E_0^D(\mathbb{Q}) = 0$，则可推出 $E_0(\mathbb{Q}(\sqrt{D}))$ 与 $E_0(\mathbb{Q})$ 同构。下面证明，在这些假设下，唯一使 $E_0(\mathbb{Q}(\sqrt{D})) \neq E_0(\mathbb{Q})$ 成立的情形是 $D = 2$。假设存在 $P \in E_0(\mathbb{Q})$，且$R \in E_0(\mathbb{Q}(\sqrt{D})) \setminus E_0(\mathbb{Q})$，使得对于某个 $n \in \mathbb{Z}$，有 $P = nR$。令 $\sigma \in \text{Gal}(\mathbb{Q}(\sqrt{D})/\mathbb{Q})$ 为非平凡自同构。于是 $P = n\,\sigma(R)$，因此 $n(R - \sigma(R)) = \mathcal{O}$。这意味着$R - \sigma(R) \in E_0(\mathbb{Q})[n]$。由于 $E_0(\mathbb{Q})_{\text{tors}} = E_0[2]$，我们得出结论：$n = 2$。

现在回顾一下，$E_0(\mathbb{Q}) = \langle T_1 \rangle \oplus \langle T_2 \rangle \oplus \langle P_0 \rangle$，其中 $T_1 = (-3,\ 0)$、$T_2 = (1,\ 0)$ 以及 $P_0 = (5,\ 8)$。因此，任意 $P \in E_0(\mathbb{Q})$ 都可以写成 $P = n_1T_1 + n_2T_2 + mP_0$，其中 $n_1,\ n_2 \in \{0, 1\}$ 和 $m \in \mathbb{Z}$。所以，只需在 $P = n_1T_1 + n_2T_2 + P_0$ 为某个 $n_1,\ n_2 \in \{0, 1\}$ 时，验证此类 R 的存在性即可。下面证明上述事实：首先，假设 $m = 2n$ 为某个 $n \neq 0$。那么我们将得到 $2(R + nP_0) = n_1T_1 + n_2T_2$，这是不可能的，因为左边具有无限阶，而右边的阶整除 2。反之，假设 $m = 2n + 1$ 为某个 $n \neq 0$。那么我们得到 $2(R + nP_0) = n_1T_1 + n_2T_2 + P_0$，这就给出了所需的关系。

最后，计算可得，$2R = n_1T_1 + n_2T_2 + P_0$, $n_1, n_2 \in \{0, 1\}$的唯一解为 $n_1 = n_2 = 0$ 和 $R = (1 + 2\sqrt{2},\ -4) + T$，其中 $T \in E[2]$。至此，证明完成。□

致谢。 Nguyen Xuan Tho还获得了越南高等数学研究院（VIASM）2025年4月至2025年5月的资助。作者衷心感谢该研究院给予的帮助和经费支持。我们感谢Xavier Xarles指出，椭圆曲线 E_1, E_4 和 E_6 属于同一个 $\mathbb{Q}$-同源类。作者感谢审稿人认真审阅稿件并提出宝贵建议。特别感谢最后一位审稿人，其详尽细致的意见极大地提升了论文的整体质量。我们由衷感谢他们所作的贡献。

本文中的所有计算均使用 Magma [2] 和 Mathematica [15]完成。

2. 设定

设 D 为无平方因子整数， K 为 $\mathbb{Q}(\sqrt{D})$ 的二次扩张。若 $S \subseteq K$，我们用 S^2 表示 S中平方数的集合。设 $a,\ b,\ c,\ d,\ e \in K$ 满足 $\left(a^2,\ b^2,\ c^2,\ d^2,\ e^2\right)$ 构成一个等差数列。则 $[a:\ b:\ c:\ d:\ e] \in V(K) \subset \mathbb{P}^4(K)$，其中 V 是由方程组定义的亏格为 5 的曲线

$$V\ :\ \{a^2+e^2=2c^2,\ a^2+c^2=2b^2,\ c^2+e^2=2d^2\}.$$

方程 $a^2+e^2=2c^2$ 具有参数化

$$[a:c:e]=\left[t^2-2t-1:t^2+1:t^2+2t-1\right] \tag{1}$$

其中 $t \in K$。将(1)应用于 V的诸方程，在不计符号的情况下，得到

$$\begin{cases} a=t^2-2t-1, \\ b=\sqrt{t^4-2t^3+2t^2+2t+1}, \\ c=t^2+1, \\ d=\sqrt{t^4+2t^3+2t^2-2t+1}, \\ e=t^2+2t-1. \end{cases} \tag{2}$$

在(2)中用 $-t$ 替换 t，得到等差数列(e^2,d^2,c^2,b^2,a^2)，等价于(a^2,b^2,c^2,d^2,e^2)，而常数等差数列对应于情形 $t=0,\pm1$。

设 $G(x)=x^4-2x^3+2x^2+2x+1$。由(2)，我们有

$$G(\pm t) \in K^2. \tag{3}$$

假设 $t \neq 0$。则

$$\frac{G(\pm t)}{t^2}=t^2+\frac{1}{t^2} \mp 2\left(t-\frac{1}{t}\right)+2=s^2 \mp 2s+4 \in K^2, \tag{4}$$

其中 $s=t-\frac{1}{t}$。由于 $s^2+4=\left(t+\frac{1}{t}\right)^2 \in K^2$，我们有

$$\begin{cases} \left(s^2+4\right)\left(s^2-2s+4\right)\left(s^2+2s+4\right) \in K^2, \\ s^2\left(s^2-2s+4\right)\left(s^2+2s+4\right) \in K^2. \end{cases}$$

设 $r=s^2$。则

$$\begin{cases} (r+4)\left(r^2+4r+16\right) \in K^2, \\ r\left(r^2+4r+16\right) \in K^2. \end{cases} \tag{5}$$

如果一个等差数列等价于常数等差数列，或其中有一个元素为 0，我们就称该等差数列为初等等差数列。表 5 给出了五个平方数的初等等差数列对应的 $t,\ s$ 和 r 的值，其中 $i=\sqrt{-1}$。

表 5：初等等差数列

t	s	r	case	$(a^2,\ b^2, c^2\ d^2, e^2)$	$[a:\ b:c:\ d:\ e]$
0	–	–	常数	(1, 1, 1, 1, 1)	$[\pm1:\ \pm1:\ \pm1:\ \pm1:\ \pm1]$
±1	0	0		$(a^2, a^2, a^2, a^2, a^2)$	$[\pm a:\ \pm a:\ \pm a:\ \pm a:\ \pm a]$
$\pm i$	$\pm2i$	-4	$c=0$	$(-2,-1,0,1,2)$	$[\pm i\sqrt{2}:\ \pm i:0:\ \pm1:\ \pm\sqrt{2}]$
$1\pm\sqrt{2}$	2	4	$a=0$	(0,1,2,3,4)	$[0:\pm1:\ \pm\sqrt{2}:\pm\sqrt{3}:\ \pm2]$
$-1\pm\sqrt{2}$	-2	4	$e=0$	(4, 3, 2, 1, 0)	$[\pm2:\ \pm\sqrt{3}:\ \pm\sqrt{2}:\ \pm1:\ 0]$
$G(t)=0$	$1\pm\sqrt{-3}$	$-2\pm2\sqrt{-3}$	$b=0$	$(-1,0,1,2,3)$	$[\pm i:0:\ \pm1:\pm\sqrt{2}:\ \pm\sqrt{3}]$

续见下页

表 5：初等等差数列（续）

$G(-t)=0$	$-1\pm\sqrt{-3}$	$-2\mp 2\sqrt{-3}$	$d=0$	$(-3,-2,-1,0,1)$	$[\pm\sqrt{3}:\ \pm\sqrt{2}:\ \pm 1:0:\ \pm i]$

注意，$b=0$ 或 $d=0$ 的情形不可能出现，因为 $\mathbb{Q}(a,\ b,\ c,\ d,\ e)=\mathbb{Q}(i,\ \sqrt{2},\ \sqrt[3]{3})$ 是一个 8次数域。

定理1和定理2的证明依赖于以下结果：

命题 6. 设 D 为无平方因子整数，K 为 $\mathbb{Q}(\sqrt{D})$ 的二次扩张。设a、b、c、d、$e\in K$满足条件：$\left(a^2\text{、}\ b^2\text{、}\ c^2\text{、}\ d^2\text{、}\ e^2\right)$ 构成由(2)给出的非初等等差数列。若秩$_{\mathbb{Z}}\,E_1^{\pm D}(\mathbb{Q})=0$，则

(1) $r\in\mathbb{Q}(\sqrt{D})$，*(2)* $s\in\mathbb{Q}(\sqrt{D})$，*(3)* $t\in\mathbb{Q}(\sqrt{D})$，*(4)* $t\in\mathbb{Q}$，若 $D\neq\pm 2$ 且秩$_{\mathbb{Z}}\,E_0^{D}(\mathbb{Q})=0$。

注。对于任意 $t\in\mathbb{Q}$，参数化 (2) 给出了由五个平方数组成的等差数列

$$((t^2-2t-1)^2,G(t),(t^2+1)^2,G(-t),(t^2+2t-1)^2),$$

也就是说，一般而言，它恰当地定义在双二次数域 $\mathbb{Q}(\sqrt{G(t)}\ \sqrt{G(-t)})$ 上。

3. Proof of Proposition 6 (1)

令 $t\in K\setminus\{0,\pm 1,\pm i,\pm 1\pm\sqrt[3]{2}\}$ 对应于 (2) 中所述的非初等等差数列，并令 $r=(t-1/t)^2$。在秩$_{\mathbb{Z}}\,E_1^{\pm D}(\mathbb{Q})=0$ 的假设下，我们证明 $r\in\mathbb{Q}(\sqrt{D})$。

假设 $r\notin\mathbb{Q}(\sqrt{D})$。于是 $K=\mathbb{Q}(\sqrt{D})(r)$。由 (5)，存在 $\alpha_1,\alpha_2,\beta_1,\beta_2\in\mathbb{Q}(\sqrt{D})$，使得

$$\begin{aligned}(r+4)\left(r^2+4r+16\right)&=(\alpha_1+\beta_1 r)^2,\\ r\left(r^2+4r+16\right)&=(\alpha_2+\beta_2 r)^2.\end{aligned}\tag{6}$$

由于 $[K:\mathbb{Q}(\sqrt{D})]=2$，$r$ 是一个二次不可约多项式 $Q(x)$ 在 $\mathbb{Q}(\sqrt{D})[x]$ 中的根。由 (6)，存在 r_1，$r_2\in\mathbb{Q}(\sqrt{D})$，使得

$$\begin{aligned}(x+4)\left(x^2+4x+16\right)-(\alpha_1+\beta_1 x)^2&=Q(x)\,(x-r_1)\,,\\ x\left(x^2+4x+16\right)-(\alpha_2+\beta_2 x)^2&=Q(x)\,(x-r_2)\,.\end{aligned}\tag{7}$$

因此，对于 $k=1,2$，有 $(r_k,\alpha_k+\beta_k\sqrt{r_k})\in C_k(\mathbb{Q}(\sqrt{D}))$，其中

$$\begin{aligned}C_1&:\ y^2=(x+4)\left(x^2+4x+16\right),\\ C_2&:\ y^2=x\left(x^2+4x+16\right).\end{aligned}$$

对于 $P_1=(x_1,y_1)\in C_1(\mathbb{Q}(\sqrt{D}))$ 和 $P_2=(x_2,y_2)\in C_2(\mathbb{Q}(\sqrt{D}))$，我们有

$$\begin{aligned}(x+4)\left(x^2+4x+16\right)-(y_1-\beta_1 x_1+\beta_1 x)^2&=Q(x)\,(x-x_1)\,,\\ x\left(x^2+4x+16\right)-(y_2-\beta_2 x_2+\beta_2 x)^2&=Q(x)\,(x-x_2)\,.\end{aligned}$$

现在，由于 $x-x_1$ 和 $x-x_2$ 整除左边的多项式，显式进行除法可得如下结果

$$\begin{aligned}Q(x)&=x^2+(8-\beta_1^2+x_1)x+32+8x_1+\beta_1^2x_1+x_1^2-2\beta_1y_1,\\ Q(x)&=x^2+(4-\beta_2^2+x_2)x+16+4x_2+\beta_2^2x_2+x_2^2-2\beta_2y_2.\end{aligned}$$

令这两个多项式相等，可得以下方程组：

$$\begin{cases} x_1\left(\beta_1^2+x_1+8\right)-2\beta_1y_1-x_2\left(\beta_2^2+x_2+4\right)+2\beta_2y_2+16=0, \\ \beta_1^2-\beta_2^2-x_1+x_2-4=0. \end{cases}$$

通过求解上述二次方程组，我们得到（β_1，β_2）。对于 $k=1$，2，设 $m_{\beta_k}(x)$ 为 β_k 的最小多项式，d_k 为 $m_{\beta_k}(x)$ 的次数。给定 D，我们列出一张表，其中对于每个点 $P_1\in C_1(\mathbb{Q}(\sqrt{D}))$ 和每个点 $P_2\in C_2(\mathbb{Q}(\sqrt{D}))$，若 d_1，$d_2\le 2$，则给出（β_1，β_2）及对应的二次多项式 $Q(x)$；否则，若不存在解（β_1，β_2），则给出 $[d_1,d_2]$ 或 $\{\}$。

对于 $k=1$，2，将 P_k 替换为 $-P_k$ 等价于将 β_k 替换为 $-\beta_k$。因此，我们在每个集合 $\{\pm P_k\}$ 中只列出一个元素。曲线 C_1 和 C_2 上的 $\mathbb{Q}(\sqrt{D})$-有理点见表 3。

- 情形 $D\neq -1$，± 3。那么

表6：情形 $D\neq -1$，± 3

P_1 \ P_2	$(0,0)$
$(-4,0)$	$(\beta_1,\ \beta_2)=(0,\ 0)$ $Q(x)=x^2+4x+16$
$(0,8)$	$(\beta_1,\ \beta_2)=(1,\ \pm\sqrt{-3})$ $Q(x)=x^2+7x+16$

情形 $(\beta_1,\beta_2)=(0,0)$ 得到 $Q(x)=x^2+4x+16$。因此，$r^2+4r+16=Q(r)=0$。于是 $r=-2\pm 2\sqrt{-3}$，这也不可能，因为它对应于初等的算术级数（见表 5）。情形 $(\beta_1,\beta_2)=(1,\pm\sqrt{-3})$ 不可能，因为 $\sqrt{-3}\notin\mathbb{Q}(\sqrt{D})$。

- 情形 $D=3$。那么

表7：情形 $D=3$

P_1 \ P_2	$(0,0)$	$(4,\ 8\sqrt{3})$
$(-4,0)$	$(0,0)$ $x^2+4x+16$	$[4,2]$
$(0,8)$	$(1,\ \pm\sqrt{-3})$ $x^2+7x+16$	$[4,4]$
$(4\pm 4\sqrt{3},\ 24\pm 16\sqrt{3})$	$[4,8]$	$[8,8]$

证明与情形 $D\neq -1$，± 3 类似。

• 情形 $D=-1$。于是

表8：情形 $D=-1$

P_1 \ P_2	(0,0)	$(\pm 4i,\ 8i)$	$(-4,\ 8i)$
$(-4,0)$	$(0,0)$ $x^2+4x+16$	$[8,4]$	$(\pm\sqrt{3},\ -i)$ x^2+x+4
$(0,8)$	$(1,\ \pm\sqrt{-3})$ $x^2+7x+16$	$[8,8]$	$[2,4]$
			$(-2,\ 2i)$ $x^2+4x+64$
			$(2,\ -2i)$ x^2+4x
$(-4\pm 4i,\ 8)$	$[4,8]$	$[4,4]$	$[8,8]$

情形 $(\beta_1,\beta_2)=(0,0)$ 和 $(\beta_1,\beta_2)=(1,\pm\sqrt{-3})$ 与情形 $D\neq -1,\pm 3$ 类似。情形 $(\beta_1,\beta_2)=(\pm\sqrt{3},-i)$ 不可能，因为 $\sqrt{3}\notin\mathbb{Q}(i)$。若 $(\beta_1,\beta_2)=(-2,2i)$，则 $Q(r)=r^2+4r+64=0$。因此，$s^4+4s^2+64=0$，这不可能，因为多项式 x^4+4x^2+64 在 $\mathbb{Q}(i)$ 上不可约。若 $(\beta_1,\beta_2)=(2,-2i)$，则 $Q(r)=r^2+4r=0$，这不可能，因为 $Q(x)$ 必须在 $\mathbb{Q}(i)$ 上不可约。

• 情形 $D=-3$。那么

表 9：情形 $D=-3$

P_1 \ P_2	(0,0)	$(-2+2\sqrt{-3},\ 0)$	$(-2-2\sqrt{-3},\ 0)$
$(-4,0)$	$(0,0)$ $x^2+4x+16$	$[4,1]$	$[4,1]$
$(0,8)$	$(1,\pm\sqrt{-3})$ $x^2+7x+16$	$[4,4]$	$[4,4]$
$(-8,\ 8\sqrt{-3})$	$[4,4]$	$[2,4]$	$[2,4]$
		$(1-\sqrt{-3},\ 0)$ $x(x+2+2\sqrt{-3})$	$(-1-\sqrt{-3},\ 0)$ $x(x+2-2\sqrt{-3})$
$(-2+2\sqrt{-3})$	$[2,4]$	$\{\}$	$[4,2]$
$(-2-2\sqrt{-3})$	$[2,4]$	$[4,2]$	$\{\}$

根据前面各情形中的同一论证，$(\beta_1,\beta_2)=(0,0)$ 这种情形不可能发生。若 $(\beta_1,\beta_2)=(1,\pm\sqrt{-3})$，则 $Q(x)=x^2+7x+16$。因此，$0=Q(s^2)=(s^2+s+4)(s^2-s+4)$。我们得到 $s=(\pm 1\pm\sqrt{-15})/2$，由此得到 t 的取值，其最小多项式为 $x^4\pm x^3+2x^2\mp x+1$。Magma 中的计算表明，$\mathbb{Q}(t)=\mathbb{Q}(\sqrt{-3},\sqrt{5})$，因此 $[\mathbb{Q}(t):\mathbb{Q}(\sqrt{-3})]=2$。然而，在这些情形下，$G(t)$ 和 $G(-t)$ 都不是 $\mathbb{Q}(t)$ 中的平方。

因此，这些情形不可能发生。若 $(\beta_1,\ \beta_2) = (\pm 1 - \sqrt{-3},\ 0)$，则 $Q(x) = x(x+2\pm 2\sqrt{-3})$，这是不可能的，因为 $Q(x)$ 必须在 $\mathbb{Q}(\sqrt{-3})$ 上不可约。

因此，$r \in \mathbb{Q}(\sqrt{D})$。

4. 命题 6 (2) 的证明

设 $t \in K \setminus \{0, \pm 1, \pm i, \pm 1 \pm \sqrt{2}\}$ 对应于 (2) 中所述的一个非初等等差数列，并设 $s = t - 1/t$。特别要注意，$s \notin \{0, \pm 2i, \pm 2\}$。我们将在假设秩$_{\mathbb{Z}} E_1^{\pm D}(\mathbb{Q}) = 0$的条件下证明$s \in \mathbb{Q}(\sqrt{D})$。

假设 $s \notin \mathbb{Q}(\sqrt{D})$。等价地，$r = s^2 \notin \mathbb{Q}(\sqrt{D})^2$。于是 $K = \mathbb{Q}(\sqrt{D})(s)$。因此，由 (4) 可得

$$s^2 \pm 2s + 4 = (\mu \pm \psi s)^2$$

其中 $\mu,\ \psi \in \mathbb{Q}(\sqrt{D})$。由命题 6 (1)，$s^2 = r \in \mathbb{Q}(\sqrt{D})$。因此，

$$r^2 + 4r + 16 = \left(s^2 - 2s + 4\right)\left(s^2 + 2s + 4\right) = \left(\mu^2 - s^2\psi^2\right)^2 = \left(\mu^2 - r\psi^2\right)^2 \in \mathbb{Q}(\sqrt{D})^2, \tag{8}$$

由于 $t^2 - st - 1 = 0$，我们有 $t = (s \pm \alpha)/2$，其中 $\alpha \in K$ 满足 $\alpha^2 = s^2 + 4 = r + 4$。

- 情形 $\alpha \in \mathbb{Q}(\sqrt{D})$。将其与 (8) 结合，得到 $(r+4)\left(r^2+4r+16\right) \in \mathbb{Q}(\sqrt{D})^2$。因此，存在 $\beta \in \mathbb{Q}(\sqrt{D})$ 使得 $(r, \beta) \in C_1(\mathbb{Q}(\sqrt{D}))$。表 3 显示，若$D \neq -1, \pm 3$ 则 $r \in \{0, -4\}$；若 $D = -1$ 则 $r \in \{0, -4, -4 \pm 4i\}$；若 $D = -3$ 则 $r \in \{0, -4, -8, -2 \pm 2\sqrt{-3}\}$；若 $D = 3$ 则 $r \in \{0, -4, 4 \pm 4\sqrt{3}\}$。情形 $r = 0$、-4、$-2 \pm 2\sqrt{-3}$ 不可能出现，因为它们对应初等等差数列（见表 5）。情形 $r = -4 \pm 4i$、-8、$4 \pm 4\sqrt{3}$ 分别给出 $r + 4 = \pm 4i$、-4、$8 \pm 4\sqrt{3}$。这些值不是相应二次域中的平方数。
- 情形 $\alpha \notin \mathbb{Q}(\sqrt{D})$。由于 $\alpha \in K = \mathbb{Q}(\sqrt{D})(s)$ 且 $[K :\ \mathbb{Q}(\sqrt{D})] = 2$，我们有 $\alpha = a + bs$，其中某个 $a, b \in \mathbb{Q}(\sqrt{D})$。由此可得 $\alpha^2 = a^2 + b^2 s^2 + 2abs$。由于 $s^2 = r \in \mathbb{Q}(\sqrt{D})$ 且 $\alpha^2 = r + 4 \in \mathbb{Q}(\sqrt{D})$，这意味着 $ab = 0$。若 $b = 0$，则 $\alpha = a \in \mathbb{Q}(\sqrt{D})$，这与我们的假设矛盾。因此 $b \neq 0$，且 $\alpha = bs$。我们得出结论 $s\alpha = as^2 = br \in \mathbb{Q}(\sqrt{D})$。于是 $r(r+4) \in \mathbb{Q}(\sqrt{D})^2$。将其与 (8) 结合，得到 $r(r+4)\left(r^2+4r+16\right) \in \mathbb{Q}(\sqrt{D})^2$。于是存在 $\beta \in \mathbb{Q}(\sqrt{D})$，使得 $(r, \beta) \in C_3(\mathbb{Q}(\sqrt{D}))$。表 3 显示，若 $D \neq -1, \pm 3$，则 $r \in \{0, -4\}$；若 $D = -1$，则 $r \in \{0, -4, -2 \pm 2i\}$；若 $D = -3$，则 $r = \{0, -4, -2, -2 \pm 2\sqrt{-3}\}$；若 $D = 3$，则 $r \in \{0, -4, -2 \pm 2\sqrt{3}\}$。情形$r = 0, -4, -2 \pm 2\sqrt{-3}$ 不可能，因为它们对应初等等差数列（见表 5）。情形 $r = -2 \pm 2i, -2, -2 + 2\sqrt{3}$ 分别得到 $r^2 + 4r + 16 = 8$、12、24。这些值在各自对应的二次域中都不是平方数，这与 (8) 矛盾。

因此，$s \in \mathbb{Q}(\sqrt{D})$。

5. 命题 6 的证明（3）

设 $t \in K \setminus \{0, \pm 1, \pm i, \pm 1 \pm \sqrt{2}\}$ 对应于（2）中所述的一个非初等等差数列。我们证明，在秩$_{\mathbb{Z}} E_1^{\pm D}(\mathbb{Q}) = 0$这一假设下，$t \in \mathbb{Q}(\sqrt{D})$

假设 $t \notin \mathbb{Q}(\sqrt{D})$。若 $s = 0$，则由 $t^2 - st - 1 = 0$可得 $t = \pm 1$，这是不可能的。因此 $s \neq 0$。于是，$t^2 = st + 1 \notin \mathbb{Q}(\sqrt{D})$。由于 $\left(t^2 - 1\right)^2 = (st)^2$，，我们得到 $t^4 = \left(s^2 + 2\right)t^2 - 1$。注意，$s^2 + 2 \neq 0$，否则 $t = (s \pm \sqrt{2})/2$，$K = \mathbb{Q}(\sqrt{-2},\ i)$ 且 $t^4 - 2t^3 + 2t^2 + 2t + 1 = \pm 2(\sqrt{2} \pm i)$ 在 K 中不是一个平方，这与（3）矛盾。由于 $t^2 \notin \mathbb{Q}(\sqrt{D})$，我们有 $t^4 = \left(s^2 + 2\right)t^2 - 1 \notin \mathbb{Q}(\sqrt{D})$。设 $w = t^4$。由于

$$t^8 - \left(s^4 + 4s^2 + 2\right)t^4 + 1 = \left(t^2 - st - 1\right)\left(t^2 + st - 1\right)\left(t^4 + \left(s^2 + 2\right)t^2 + 1\right) = 0,$$

w 是.....的一个根

$$F(x) = x^2 - \left(s^4 + 4s^2 + 2\right)x + 1 \in \mathbb{Q}(\sqrt{D})[x]. \tag{9}$$

由于 $w \notin \mathbb{Q}(\sqrt{D})$ $F(x)$ 在 $\mathbb{Q}(\sqrt{D})[x]$ 中是不可约的，且 $K = \mathbb{Q}(\sqrt{D},\ w)$。由（3）可得，

$$t^8 + 14t^4 + 1 = \left(t^4 - 2t^2 + 2t^2 + 2t + 1\right)\left(t^4 + 2t^2 + 2t^2 - 2t + 1\right) \in K^2.$$

因此，

$$w\left(w^2 + 14w + 1\right) = t^4\left(t^8 + 14t^4 + 1\right) \in K^2.$$

因此，存在 $\alpha,\ \beta \in \mathbb{Q}(\sqrt{D})$ 使得

$$w\left(w^2 + 14w + 1\right) = (\alpha + \beta w)^2.$$

于是存在 $\omega_0 \in \mathbb{Q}(\sqrt{D})$ 使得

$$x\left(x^2 + 14x + 1\right) - (\alpha + \beta x)^2 = F(x)\,(x - \omega_0).$$

因此，$(\omega_0,\ \alpha + \beta\omega_0)$ 是椭圆曲线 C_4：$y^2 = x\left(x^2 + 14x + 1\right)$ 上的一个 $\mathbb{Q}(\sqrt{D})$-有理点。对于任意点 $P = (x_0,\ y_0) \in C_4(\mathbb{Q}(\sqrt{D}))$，有

$$x\left(x^2 + 14x + 1\right) - (y_0 - \beta x_0 + \beta x)^2 = F_\beta(x)\,(x - x_0). \tag{10}$$

设 $(0,\ 0) \in C_4(\mathbb{Q}(\sqrt{D}))$。于是得到 $F_\beta(x) = x^2 + (14 - \beta^2)x + 1$。与 (9) 比较可得 $14 - \beta^2 = -\left(s^4 + 4s^2 + 2\right)$。因此 $s^4 + 4s^2 + 16 = \beta^2$。于是 $(s,\ \beta)$ 是曲线 C_5：$y^2 = x^4 + 4x^2 + 16$ 上的一个 $\mathbb{Q}(\sqrt{D})$-有理点。根据表 3，我们得到 $s \in \{0, \pm 2, \pm 2i, \pm 1 \pm \sqrt{-3}\}$，这对应于初等等差数列（见表 5）。

令 $(1,\ \pm 4) \in C_4(\mathbb{Q}(\sqrt{D}))$。于是得到 $F_\beta(x) = x^2 + (15 - \beta^2)x + (4 + \beta)^2$。与 (9) 比较可得 $(\beta,\ s)$，其中 $\beta = -3,\ -5$，而 s 的最小多项式分别为 $x^4 + 4x^2 + 8$ 和 $x^4 + 4x^2 - 8$，这是不可能的，因为 $s \in \mathbb{Q}(\sqrt{D})$。

利用表 4 中的数据，我们详细列出表 10。对于每个 $P \in C_4(\mathbb{Q}(\sqrt{D}))$，表中给出了 $P \notin C_4(\mathbb{Q})$，以及通过将 (9) 与 (10) 比较，由等式 $F_\beta(x) = F(x)$ 得到的解 β。注意，将 P 替换为 $-P$ 等价于将 β 改为 $-\beta$。因此，集合 $\{\pm P\}$ 中只展示一个元素。

表 10：

P	β
$(-3 + 2\sqrt{2},\ \ 8 - 6\sqrt{2})$	$\pm i + (2 \pm i)\sqrt{2} \notin \mathbb{Q}(\sqrt{2})$
$(-3 - 2\sqrt{2},\ \ +8 + 6\sqrt{2})$	$\pm i + (2 \mp i)\sqrt{2} \notin \mathbb{Q}(\sqrt{2})$
$(-7 \pm 4\sqrt{3},\ 0)$	$\pm i(2 + \sqrt{3}) \notin \mathbb{Q}(\sqrt{3})$

表 10 显示，在所有情况下，$\beta \notin \mathbb{Q}(\sqrt{D})$。这就完成了 $t \in \mathbb{Q}(\sqrt{D})$的证明。

6. 命题 6 (4) 的证明

设 $D \neq \pm 2$ 是一个无平方因子整数，满足 $\operatorname{rank}_{\mathbb{Z}} E_1^{\pm D}(\mathbb{Q}) = 0$ 且 $\operatorname{rank}_{\mathbb{Z}} E_0^{D}(\mathbb{Q}) = 0$。令 $t \in K \setminus \{0, \pm 1, \pm i, \pm 1 \pm \sqrt{2}\}$ 对应于 (2) 中所述的一个非初等等差数列。我们证明 $t \in \mathbb{Q}$。由于 $[K:\ \mathbb{Q}(\sqrt{D})] = 2$，存在 $\alpha \in K$ 使得 $\alpha^2 \in \mathbb{Q}(\sqrt{D})$ 且 $K = \mathbb{Q}(\sqrt{D},\ \alpha)$。由 (3)，存在 $\gamma_1,\ \delta_1,\ \gamma_2,\ \delta_2 \in \mathbb{Q}(\sqrt{D})$，使得

$$\begin{cases} t^4 - 2t^3 + 2t^2 + 2t + 1 = (\delta_1 + \gamma_1\alpha)^2, \\ t^4 + 2t^3 + 2t^2 - 2t + 1 = (\delta_2 + \gamma_2\alpha)^2. \end{cases} \tag{11}$$

由于 $t \in \mathbb{Q}(\sqrt{D})$ 和 $\alpha \notin \mathbb{Q}(\sqrt{D})$，我们得到 $\gamma_1\delta_1 = \gamma_2\delta_2 = 0$。共有四种情况：

- $\gamma_1=\gamma_2=0$。则
$$t^8+14t^4+1=\left(t^4-2t^3+2t^2+2t+1\right)\left(t^4+2t^3+2t^2-2t+1\right)=(\delta_1\delta_2)^2\in\mathbb{Q}(\sqrt{D})^2.$$
因此 $\left(t^2,\ \delta_1\delta_2\right)$ 是曲线 $C_6:\ y^2=x^4+14x^2+1$上的一个 $\mathbb{Q}(\sqrt{D})$-点。由表 3，我们有
$$C_6(\mathbb{Q}(\sqrt{D}))=C_6(\mathbb{Q})=\{(0,\pm1),(\pm1,\pm4)\}$$
对于任意满足秩$_{\mathbb{Z}}\,E_1^D(\mathbb{Q})=0$ 的整数 D。因此，$t\in\{0,\pm1\}$，这与假设不符。

- $\delta_1=\delta_2=0$。则
$$t^8+14t^4+1=\left(t^4-2t^3+2t^2+2t+1\right)\left(t^4+2t^3+2t^2-2t+1\right)=\left(\alpha^2\gamma_1\gamma_2\right)^2\in\mathbb{Q}(\sqrt{D})^2.$$
因此 $\left(t^2,\ \alpha^2\gamma_1\gamma_2\right)\in C_6(\mathbb{Q}(\sqrt{D}))$，这由与情形$\gamma_1=\gamma_2=0$类似的论证可知是不可能的。

- $\gamma_1=\delta_2=0$。(11) 的第一个方程表明 $t^4-2t^3+2t^2+2t+1=\delta_1^2$。因此，$(t,\ \delta_1)$ 是曲线 $C_0:\ y^2=x^4-2x^3+2x^2+2x+1$ 上的一个 $\mathbb{Q}(\sqrt{D})$ 点。由引理 5 可知，对于任意满足 $\operatorname{rank}_{\mathbb{Z}}E_0^D(\mathbb{Q})=0$ 的无平方因子整数 $D\neq\pm2$，都有$C_0(\mathbb{Q}(\sqrt{D}))=C_0(\mathbb{Q})$。于是$t\in\mathbb{Q}$。
- $\delta_1=\gamma_2=0$。(11) 的第二个方程表明 $t^4+2t^3+2t^2-2t+1=\delta_2^2$。因此，$(-t,\ \delta_2)$ 是曲线 C_0 上的一个 $\mathbb{Q}(\sqrt{D})$ 点。与情形 $\gamma_1=\delta_2=0$ 类似，我们得到：如果 $D\neq\pm2$，那么 $t\in\mathbb{Q}$。

因此，如果 $D\neq\pm2$，那么 $t\in\mathbb{Q}$。

7. 定理1和定理2的证明

设 D 是一个无平方因子整数，满足秩$_{\mathbb{Z}}\,E_1^{\pm D}(\mathbb{Q})=0$，且 K 是 $\mathbb{Q}(\sqrt{D})$ 的一个二次扩张。设 $(a^2,\ b^2,\ c^2,\ d^2,\ e^2)$ 是在 K 上恰当定义的五个平方数的等差数列。若 $(a^2,\ b^2,\ c^2,\ d^2,\ e^2)$ 是初等但非恒定的，那么它等价于以下某一数列

- $(-2,\ -1,\ 0,\ 1,\ 2)$，且 $K=\mathbb{Q}(i,\sqrt{2})$。特别地，$D=-1,\ \pm2$。
- $(0,\ 1,\ 2,\ 3,\ 4)$，且 $K=\mathbb{Q}(\sqrt{3},\sqrt{2})$。特别地，$D=2,\ 3$。注意，等差数列 $(4,\ 3,\ 2,\ 1,\ 0)$ 等价于 $(0,\ 1,\ 2,\ 3,\ 4)$。

现在假设 $(a^2,\ b^2,\ c^2,\ d^2,\ e^2)$ 不是一个初等的等差数列。根据命题 6 (3)，存在 $t\in\mathbb{Q}(\sqrt{D})$，使得 $(a^2,\ b^2,\ c^2,\ d^2,\ e^2)$ 等价于该等差数列
$$((t^2-2t-1)^2,\beta^2,(t^2+1)^2,\gamma^2,(t^2+2t-1)^2),$$
其中 $\beta^2=G(t)$ 和 $\gamma^2=G(-t)$，且 $G(x)=x^4-2x^3+2x^2+2x+1$。

我们来证明定理1：

(A) 假设 $\operatorname{rank}_{\mathbb{Z}}E_0^D(\mathbb{Q})=0$。由于 $D\neq\pm2$。根据命题 6 (4)，我们有 $t\in\mathbb{Q}$。在这种情况下，我们有 $C_0(\mathbb{Q}(\sqrt{D}))=C_0(\mathbb{Q})$。因此，如果 $G(t)$ 的值是 $\mathbb{Q}(\sqrt{D})$ 上的平方，那么它已经是 $\mathbb{Q}$ 上的平方。于是，等差数列的五项中有四项定义在 $\mathbb{Q}$上，因此，这个由五项组成的完整等差数列恰当地定义在 $\mathbb{Q}$ 的二次扩张上。

（B）假设秩$_{\mathbb{Z}}\,E_0^D(\mathbb{Q})\neq0$，且 $\mathbb{Q}(\sqrt{D})$的类数为1。由命题 6（3），我们有 $t\in\mathbb{Q}(\sqrt{D})$。由于 $\mathbb{Q}(\sqrt{D})$的整数环是唯一分解整环，存在 $\alpha,\delta\in\mathbb{Q}(\sqrt{D})$，使得 $G(-t)=\alpha\,\delta^2$。我们可以断定 α 在 $\mathbb{Q}(\sqrt{D})$中不是平方，否则在 $\mathbb{Q}(\sqrt{D})$中将存在非平凡五个平方数等差数列。然而这是不可能的，因为 [9, 命题 5.2]指出，一个必要条件是秩$E_1^{\pm D}(\mathbb{Q})\geq2$。于是等差数列（$a^2,b^2,c^2,d^2,e^2$）在 $K=\mathbb{Q}(\sqrt{D},\omega)$上被恰当定义，其中 $\omega^2=\alpha$。

现在，在假设（a^2,b^2,c^2,d^2,e^2）不是初等等差数列的条件下，定理 2 的证明：

- $D\in\{-1,3\}$：由于秩$_{\mathbb{Z}}\,E_0^D(\mathbb{Q})=0$ 和 $D\neq\pm2$，证明与情形（A）类似。

• $D = \pm 2$: 在这种情况下，秩$_{\mathbb{Z}}\, E_0^D(\mathbb{Q}) = 0$。由命题 6 (3)，我们有 $t \in \mathbb{Q}(\sqrt{D})$。由于 $\mathbb{Q}(\sqrt{D})$的类数为 1，证明与情形（B）类似。

8. 定理3的证明

我们可以将定理3视为定理1和定理2的推论。设 D 为一个无平方因子整数，满足 rank$_{\mathbb{Z}}\, E_1^{\pm D}(\mathbb{Q}) = 0$，且 K 是 $\mathbb{Q}(\sqrt{D})$的二次扩张。我们将证明，在 K 上恰当定义的五个平方数等差数列无法扩展为长度为6的数列。

设 $(a^2,\ b^2,\ c^2,\ d^2,\ e^2,\ f^2)$ 是在 K上恰当定义的六个平方数等差数列。那么，$(a^2,\ b^2,\ c^2,\ d^2,\ e^2)$ 或 $(b^2,\ c^2,\ d^2,\ e^2,\ f^2)$ 是在 K上恰当定义的五个平方数等差数列。假设 $D \neq -1,\ \pm 2,\ 3$。我们可以应用定理1：

(A) 假设 rank$_{\mathbb{Z}}\, E_0^D(\mathbb{Q}) = 0$，那么在 K 上恰当定义的六个平方数的非恒定等差数列不存在，因为长度为五的数列也不存在。(B) 假设 rank$_{\mathbb{Z}}\, E_0^D(\mathbb{Q}) \neq 0$，且 $\mathbb{Q}(\sqrt{D})$ 的类数为 1。设 $(a^2, b^2, c^2, d^2, e^2)$ 是在 K 上恰当定义的五个平方数的等差数列（另一种情况完全等价）。那么存在 $x_1, x_2, x_3, x_4, x_5, \alpha \in \mathbb{Q}(\sqrt{D})$，且 α 是非平方数，使得 $(a^2, b^2, c^2, d^2, e^2)$ 等价于 $(x_1^2, x_2^2, x_3^2, \alpha\, x_4^2, x_5^2)$。设 $s \in \mathbb{Q}(\sqrt{D})$ 满足

$$(sa^2, sb^2, sc^2, sd^2, se^2) = (x_1^2, x_2^2, x_3^2, \alpha\, x_4^2, x_5^2).$$

由等式 $sa^2 = x_1^2$ 和 $sd^2 = \alpha\, x_4^2$，我们得到 $\alpha \in \mathbb{Q}(\sqrt{D})^2$，这与假设矛盾。对于 $D = -1,\ 3,\ \pm 2$ 的情形，我们应用定理 2：

• 如果 $D = -1$，那么 $K = \mathbb{Q}(i,\ \sqrt{2})$，并且在 K 上恰当定义的唯一非恒定五个平方数的等差数列，在等价意义下为（$-2,\ -1,\ 0,\ 1,\ 2$）。因此，将其延拓为长度为6的等差数列只有两种方式：

$$(-3, -2, -1, 0, 1, 2) \qquad \text{and} \qquad (-2, -1, 0, 1, 2, 3).$$

然而，这两种可能性都不成立，因为它们将意味着 $\sqrt{-3} \in K$ 或 $\sqrt{-3} \in K$。

• 如果 $D = 3$，那么 $K = \mathbb{Q}(\sqrt{3},\ \sqrt{2})$，并且在 K 上恰当定义的唯一非恒定五个平方数的等差数列，在等价意义下为（$0,\ 1,\ 2,\ 3,\ 4$）。类似于前一种情形的论证将导致 $i \in K$ 或 $\sqrt{5} \in K$，这同样会产生矛盾。

• 如果 $D = 2$，那么有三种可能性。前两种分别是 $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$且五个平方数的等差数列为（$0, 1, 2, 3, 4$），或者 $K = \mathbb{Q}(\sqrt{2}, i)$且（$-2, -1, 0, 1, 2$）。随后，证明分别与情形 $D = -1$ 和 $D = 3$ 中的证明相同。最后一种情形是 $K = \mathbb{Q}(\sqrt{2}, \sqrt{\alpha})$，其中 $\left(a^2, b^2, c^2, \alpha\, d^2, e^2\right)$，且 $a, b, c, d, e, \alpha \in \mathbb{Q}(\sqrt{2})$，并且 α 为非平方数。在这种情况下，证明与情形$D \neq -1, \pm 2, 3$ 中的证明相同，应用定理 1 (B)

• 如果 $D = -2$，那么 $K = \mathbb{Q}(i, \sqrt{-2})$，五个平方数的等差数列等价于 $(-2, -1, 0, 1, 2)$，且证明与 $D = -1$ 的情形相同；或者 $K = \mathbb{Q}(\sqrt{-2}, \sqrt{\alpha})$，其中$\left(a^2, b^2, c^2, \alpha\, d^2, e^2\right)$，这里 $a, b, c, d, e, \alpha \in \mathbb{Q}(\sqrt{-2})$，且 α 是非平方数。在这种情况下，利用定理1 (B)，可以按照 $D \neq -1, \pm 2, 3$ 的情形以相同方式进行论证。

9. $\mathbb{Q}(\sqrt{-2})$ 和 $\mathbb{Q}(\sqrt{2})$ 情形下的参数化

设 D 为一个无平方因子整数，使得 rank$_{\mathbb{Z}}\, E_1^{\pm D}(\mathbb{Q}) = 0$。我们已经证明，在 $\mathbb{Q}(\sqrt{D})$ 的二次扩张上，任意非初等的五个平方数的等差数列都等价于

$$\left((t^2 - 2t - 1)^2,\ \beta^2,\ (t^2 + 1)^2,\ \alpha\delta^2,\ (t^2 + 2t - 1)^2\right),$$

其中 $t,\ \alpha,\ \beta,\ \delta \in \mathbb{Q}(\sqrt{D})$ 满足 $\beta^2 = G(t)$ 和 $\alpha\delta^2 = G(-t)$。特别地，对于任意五个平方数的非初等等差数列，都存在一个点 $R \in E_0(\mathbb{Q}(\sqrt{D}))$，反之亦然。请注意，这种对应并非一一对应。此构造还原了 [9]中针对特殊情形 $D = 1$ 所发展的构造。也就是说，对于任意 $R \in E_0(\mathbb{Q})$，我们都能得到一个二次域上的五个平方数的等差数列，

但当 $R \in E_0(\mathbb{Q})_{\mathrm{tors}}$ 时除外，此时该数列是平凡的。请注意，秩$_{\mathbb{Z}} E_1^{\pm 1}(\mathbb{Q}) = 0$。令 $T_1 = (-3,\ 0)$、$T_2 = (1,\ 0)$ 和 $P = (0,\ 3)$，则

$$E_0(\mathbb{Q}) = \langle T_1 \rangle \oplus \langle T_2 \rangle \oplus \langle P \rangle.$$

若 $n \in \mathbb{Z}$, $n \geq 0$，点集 $S_n = \{n_1 T_1 + n_2 T_2 + mP\colon\ n_1, n_2 \in \{0,1\}, m \in \{n, -n-1\}\}$对应于同一个五个平方数的等差数列（相差一个等价变换）。例如，若$n = 1$ 集合 S_1 对应于等差数列 $(7^2, 13^2, 17^2, (\sqrt{409})^2, 23^2)$。

若 $D \neq \pm 2$ 使得秩$_{\mathbb{Z}} E_0^D(\mathbb{Q}) = 0$，则 $E_0(\mathbb{Q}(\sqrt{D})) = E_0(\mathbb{Q})$。那么$E_0(\mathbb{Q}(\sqrt{D}))$中的任意点 R 都对应于有理数域$\mathbb{Q}$的一个二次扩张上的五个平方数的等差数列。因此，它在有理数域 $\mathbb{Q}(\sqrt{D})$的二次扩张上未被恰当定义。

让我们简要研究 $D = -2$ 和 $D = 2$的情形。首先， $D = -2$。我们有

$$E_0(\mathbb{Q}(\sqrt{-2})) = \langle T_1 \rangle \oplus \langle T_2' \rangle \oplus \langle P \rangle,$$

其中 $T_2' = (1 - 2\sqrt{-2},\ 4 + 4\sqrt{-2})$ 满足 $2T_2' = T_2$。在这种情况下，如果 $n \in \mathbb{Z}$, $n \geq 0$，点集 $\{n_1 T_1 + n_2 T_2' + mP\colon\ n_1 \in \{0,1\},\ n_2 \in \{1,3\},\ m \in \{n, -n-1\}\}$ 在等价意义下对应于同一个五个平方数的等差数列。表12给出了 $n = 0$，1，2，3所对应的五个平方数的等差数列。

表11：等差数列示例。

n	等差数列
0	$(2^2,\ 1^2,\ -2,\ -5,\ -2 \cdot 2^2)$
1	$(34^2, 23^2, -2 \cdot 7^2, -29 \cdot 5^2, -2 \cdot 26^2)$
2	$(5986^2, 647^2, -2 \cdot 4183^2, -70408565, -2 \cdot 7274^2)$
3	$(25953218^2, 18240049^2, -2 \cdot 2021231^2, -349040886543845, -2 \cdot 18572978^2)$

这些等差数列的形式为 $\left(a^2,\ b^2,\ -2c^2,\ -md^2,\ -2e^2\right)$，其中 $a,\ b,\ c,\ d,\ e,\ m \in \mathbb{Z}$，且 $m > 0$ 为无平方因子。特别地，它们在 $K = \mathbb{Q}(\sqrt{-2},\ \sqrt{-m})$上被恰当地定义。我们已对 $0 \leq n \leq 11$验证了上述断言。这些计算结果支持猜想 4 (i)。

在 $D = 2$的情况下，我们有

$$E_0(\mathbb{Q}(\sqrt{2})) = \langle T_1 \rangle \oplus \langle T_2 \rangle \oplus \langle P' \rangle,$$

其中 $P' = (1 + 2\sqrt{2},\ 4)$满足 $2P' + T_1 = -P$。在此情况下，若 $n \in \mathbb{Z}$、 $n > 0$为奇数，则点集 $S_n = \{n_1 T_1 + n_2 T_2 + mP'\colon\ n_1,\ n_2 \in \{0,1\},\ m \in \{n, -n-2\}\}$ 对应于同一个五个平方数的等差数列（在等价意义下）。表12给出了 $n = 1,\ 3,\ 5$所对应的五个平方数的等差数列。

表12：等差数列示例。

n	等差数列
1	$(2 \cdot 4^2,\ 5^2, 2 \cdot 3^2, 11, 2^2)$
3	$(2 \cdot 120^2, 241^2, 2 \cdot 209^2, 3 \cdot 5 \cdot 659, 382^2)$
5	$(2 \cdot 142324^2, 221285^2, 2 \cdot 169443^2, 11 \cdot 10691 \cdot 560171, 272638^2)$

在这些情况下，等差数列的形式为 $\left(2a^2、\ b^2、\ 2c^2、\ m、\ e^2\right)$，其中 $a、\ b、\ c、\ d、\ e、\ m \in \mathbb{Z}$，且 $m > 0$ 无平方因子。特别地，它们在 $K = \mathbb{Q}(\sqrt{2}、\ \sqrt{m})$ 上被恰当定义。我们已检验上述断言对 $0 \leq n \leq 21$ 为奇数的情形成立。这些计算支持猜想 4 (ii)。

参考文献

[1] 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。[2] W. Bosma、J. Cannon 和 C. Playoust，《Magma 代数系统。I. 用户语言》，J. Symbolic Comput. 24(1997)，第 3-4 期，235-265。[3] A. Bremner 和 S. Siksek，《三次域中的等差数列平方数》，Int. J. Number Theory 12 (2016)，第 5 期，1409-1414。[4] D. K. Faddeev，《由方程 $x^4+y^4=1$定义的曲线上的因子类群》，《苏联数学文献》1 (1960)，1149-1151；《苏联科学院院刊》134 (1960)，776-777（俄文原版）。[5] E. Gonz´alez-Jim´enez 和 F. Najman，《基变换下椭圆曲线的挠点增长》，Math. Comp. 89 (2020)，1457-1485。[6] E. Gonz´alez-Jim´enez 和 F. Najman，《确定椭圆曲线挠点增长的算法》，Exp. Math. 32 (2023)，70-81。[7] E. Gonz´alez-Jim´enez 和 J.M. Tornero，《有理椭圆曲线在二次域上的挠点》，Rev. R. Acad. Cienc. Exactas F´is. Nat. Ser. A Math. RACSAM 108 (2014)，923-934。[8] E. Gonz´alez-Jim´enez 和 J.M. Tornero，《有理椭圆曲线在二次域上的挠点 II》，Rev. R. Acad. Cienc. Exactas F´is. Nat. Ser. A Math. RACSAM 110 (2016)，121-143。[9] E. Gonz´alez-Jim´enez 和 X. Xarles，《二次域中的五个平方数等差数列》，Rev. Mat. Iberoam. 29 (2013)，第 4 期，1211-1238。[10] K. Kramer，《二次扩张下椭圆曲线的算术》，Trans. Am. Math. Soc. 264 (1981) 121-135。[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] F. Najman，《有理椭圆曲线在三次域上的挠点及 $X_1(N)$ 上的零星点》，Math. Res. Letters, 23 (2016) 245-272。[13] LMFDB 协作组，《L 函数与模形式数据库》，https://www.lmfdb.org, 2024, [在线；访问日期： 2024] 年 4 月 15 日。[14] X. Xarles，《数域中的等差数列平方数》，J. Number Theory 132 (2012)，第 3 期，379-389。[15] Wolfram Research, Inc.，《Mathematica》，12.1 版，Champaign, IL (2020)。

马德里自治大学，数学系，马德里，西班牙电子邮箱：enrique.gonzalez.jimenez@uam.es

河内科技大学，河内，越南电子邮箱：tho.nguyenxuan1@hust.edu.vn