arXiv:2305.05851v1 [math.NT] 10 May 2023

四椭圆模曲线 $X_1(N)$

全大烈

Abstract. 本文确定了有理数域 $\mathbb{Q}$ 上所有四椭圆模曲线 $X_1(N)$，并为这些四椭圆曲线 $X_1(N)$ 找到了一些从 $X_1(N)$ 到椭圆曲线的四椭圆映射 ϕ_N。此外，我们将把 ϕ_N 显式构造为有理函数。而且，我们将证明所找到的所有 ϕ_N 都是伽罗瓦的，并利用循环映射 ϕ_{17}，找出在循环四次扩域上挠子群为 $\mathbb{Z}/17\mathbb{Z}$ 的椭圆曲线。

1. Introduction

设 X 是数域 K 上亏格为 $g(X) \geq 2$ 的光滑射影曲线。假设存在一个次数为 d 的映射 $\phi\colon X \to E$，其中目标曲线是某条椭圆曲线 E。那么，当 $d = 2$ 分别为 2、3 和 4 时，称 X 为双椭圆、三椭圆和四椭圆曲线。

对于正整数 N，模曲线 $X_1(N)$（去掉尖点后）参数化了对 (E, P) 的同构类，其中 E 是一条椭圆曲线，P 是 E 上阶为 N 的挠点。

第一作者和 Kim [JK] 确定了所有双椭圆曲线 $X_1(N)$。最近，作者 [J]确定了 $\mathbb{Q}$ 上的所有三椭圆曲线 $X_1(N)$，也就是说，它们存在从 $X_1(N)$ 到 E 上的椭圆曲线的 $\mathbb{Q}$-有理三椭圆映射，次数为 3。此外，他构造了从 $X_1(N)$ 上的三椭圆 $\mathbb{Q}$-有理三椭圆映射到椭圆曲线的显式例子。有趣的是，他在构造从 $X_1(21)$ 到椭圆曲线的三椭圆映射时，重新发现了 Najman 的椭圆曲线 162B1，它定义在 $\mathbb{Q}(\zeta_9)^+$ 上，是一条带有 $\mathbb{Z}/21\mathbb{Z}$ 挠点的三次数域上的椭圆曲线。事实上，椭圆曲线 162B1 对应于 $X_1(21)$ 上的一个 3 次孤立点。一般而言，若 $X_1(N)$ 上的一个点定义在一个相对于 $\mathbb{Q}$ 次数为 n 的数域上，则称其为次数为 n 的点。特别地，我们称次数为 4 的点为四次点。

本文确定了有理数域 $\mathbb{Q}$ 上所有的四椭圆模曲线 $X_1(N)$，并为这些四椭圆模曲线 $X_1(N)$ 找出了一些从四椭圆曲线 $X_1(N)$ 到椭圆曲线的四椭圆映射 ϕ_N。我们还将把 ϕ_N 显式构造为有理函数。从计算角度来看，显式构造从高亏格代数曲线到椭圆曲线的映射似乎很有意义。至少作者没有找到任何文献展示这些显式表达式，除了作者之前的工作 [J]。此外，我们证明了找到的所有 ϕ_N 都是伽罗瓦的，并利用循环映射 ϕ_{17} 找到了循环四次扩域上的挠子群为 $\mathbb{Z}/17\mathbb{Z}$ 的椭圆曲线。

我们的主要定理如下：

本研究由韩国教育部资助的韩国国家研究基金会（NRF）基础科学研究计划支持（2019R1F1A1060149, 2022R1A2C1010487）。2020 *Mathematics Subject Classification*：11G18，11G30*Keywords*：四椭圆模曲线；四椭圆映射

定理 1.1. $X_1(N)$ 在 $\mathbb{Q}$ 上是四椭圆的，当且仅当 $N = 17$、20、24、26、28、30、32。此外，它们都有 $\mathbb{Q}$ 有理的伽罗瓦四椭圆映射，即它们存在从 $X_1(N)$ 到椭圆曲线的 $\mathbb{Q}$ 有理伽罗瓦 4 次映射。特别地，对于 $N = 17$、20、26、30 和 32，它们是循环的，其余则不是。

我们还想对椭圆曲线的挠子群补充几点说明。众所周知，Mazur [M] 确定了有理数域 $\mathbb{Q}$ 上椭圆曲线的挠子群所有可能的群结构。Kamienny [K], Kenku 和 Momose [KM] 完成了与 Mazur 相同的工作，将其结果推广到了二次数域上。

在这些结果之后，研究重点转向了次数更高的数域。Jeon、Kim 和 Schweizer [JKS1] 找出了遍历所有三次数域上的椭圆曲线时会无限多次出现的所有挠群，如下所示:

$$\begin{array}{ll} \mathbb{Z}/N\mathbb{Z}, & N = 1-16, 18, 20, \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2N'\mathbb{Z}, & N' = 1-7. \end{array} \tag{1.1}$$

自 Najman 的椭圆曲线在 [N], 被发现后， [W] 正式提出猜想：三次数域上椭圆曲线的唯一可能挠群就是 (1.1) 中的那些以及 $\mathbb{Z}/21\mathbb{Z}$。最终，Derickx、Etropolski、van Hoeij、Morrow 和 Zureick-Brown [DE] 证明了这一猜想，因此，三次数域上椭圆曲线的挠群 $E(K)_{tors}$ E 必须同构于以下 26 种类型之一:

$$\begin{array}{ll} \mathbb{Z}/N\mathbb{Z}, & N = 1-16, 18, 20, 21 \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2N'\mathbb{Z}, & N' = 1-7. \end{array} \tag{1.2}$$

在四次数域 K 上， [JKP]证明了，无穷多次出现为挠群 $E(K)_{\mathrm{tors}}$ 的群结构恰好是以下 38 种:

$$\begin{array}{ll} \mathbb{Z}/N_1\mathbb{Z}, & N_1 = 1-18, 20, 21, 22, 24 \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2N_2\mathbb{Z}, & N_2 = 1-9 \\ \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3N_3\mathbb{Z}, & N_3 = 1-3 \\ \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4N_4\mathbb{Z}, & N_4 = 1-2 \\ \mathbb{Z}/5\mathbb{Z} \oplus \mathbb{Z}/5\mathbb{Z}, & \\ \mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}, & \end{array} \tag{1.3}$$

其中 K 遍历所有四次数域， E 遍历所有定义在 K 上的椭圆曲线。至于四次数域，目前尚未得到挠子群的完整分类。与三次数域不同，尚未发现 $X_1(N)$ 上次数为 4 的稀疏点，因此 (1.3) 仍有可能构成四次数域上的完整分类；这一结果最终会如何，十分值得关注。

最后，我们将对我们在循环四次扩域上构造具有挠子群$\mathbb{Z}/17\mathbb{Z}$ 的椭圆曲线作出一些说明。Chou [C] 证明，如果 E 是定义在 $\mathbb{Q}$上的椭圆曲线，且 K 是 $\mathbb{Q}$的伽罗瓦四次扩张，那么 $E(K)_{\mathrm{tors}}$ 属于以下27种类型之一:

$$\begin{array}{ll} \mathbb{Z}/N_1\mathbb{Z}, & N_1 = 1-16, N_1 \neq 11, 14 \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2N_2\mathbb{Z}, & N_2 = 1-6, 8 \\ \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3N_3\mathbb{Z}, & N_3 = 1, 2 \\ \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4N_4\mathbb{Z}, & N_4 = 1, 2 \\ \mathbb{Z}/5\mathbb{Z} \oplus \mathbb{Z}/5\mathbb{Z}, & \\ \mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}, & \end{array} \tag{1.4}$$

上述结果表明，我们的挠点为 $\mathbb{Z}/17\mathbb{Z}$ 的椭圆曲线在循环四次扩域上不存在 $\mathbb{Q}$-有理魏尔斯特拉斯方程。

2. Preliminaries

令 $\Gamma(1) = \mathrm{SL}_2(\mathbb{Z})$ 为全模群。对于任意正整数 N，我们有 $\Gamma(1)$ 的子群$\Gamma(N)$、 $\Gamma_1(N)$ 和 $\Gamma_0(N)$，它们分别由满足模 N同余于 $\left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right)$、$\left(\begin{smallmatrix}1&*\\0&1\end{smallmatrix}\right)$ 和 $\left(\begin{smallmatrix}*&*\\0&*\end{smallmatrix}\right)$ 的矩阵 $\left(\begin{smallmatrix}a&b\\c&d\end{smallmatrix}\right)$ 定义。我们令 $X(N)$、 $X_1(N)$ 和 $X_0(N)$ 分别表示与 $\Gamma(N)$、 $\Gamma_1(N)$ 和 $\Gamma_0(N)$ 相关联、定义在 $\mathbb{Q}$ 上的模曲线。另有一些模曲线 $X_\Delta(N)$ 与 $\Gamma_0(N)$ 的子群 $\Gamma_\Delta(N)$ 相关联，这些子群由满足 $a \in \Delta$的矩阵 $\left(\begin{smallmatrix}a&b\\c&d\end{smallmatrix}\right)$ 定义，其中 Δ是 $(\mathbb{Z}/N\mathbb{Z})^*$ 的一个包含 -1的子群。对于 $\Delta = \{\pm 1\}$，这就是 $X_1(N)$。

现在我们介绍椭圆曲线的一种特殊形式，该形式常用于描述一对 (E, P)，其对应于 $X_1(N)$ 的非尖点（参见 [H]）。具有点 $P = (0,0)$ 的椭圆曲线的 Tate 正规形为

$$E = E(b,c) : Y^2 + (1-c)XY - bY = X^3 - bX^2,$$

当且仅当 $b \neq 0$ 时，此曲线是非奇异的。在曲线 $E(b,c)$ 上，我们可以使用弦切法推导出如下结论:

$$\begin{aligned}
P =& (0,\ 0),\\
2P =& (b,\ bc),\\
3P =& (c,\ b-c),\\
4P =& \big(r(r-1),\ r^2(c-r+1)\big);\quad b = cr,\\
5P =& \big(rs(s-1),\ rs^2(r-s)\big);\quad c = s(r-1),\\
6P =& \left(\frac{s(r-1)(r-s)}{(s-1)^2},\ \frac{s^2(r-1)^2(rs-2r+1)}{(s-1)^3}\right)
\end{aligned} \tag{2.1}$$

条件 $NP = O$in $E(b,c)$ 给出了 $X_1(N)$ 的定义方程。例如， $11P = O$意味着 $5P = -6P$，因此

$$X_{5P} = X_{-6P} = X_{6P},$$

其中， X_{nP} 表示 P的 n 倍点 nP 的 X 坐标。(2.1) 意味着

$$rs(s-1) = \frac{s(r-1)(r-s)}{(s-1)^2}. \tag{2.2}$$

不失一般性，可以排除 $s = 0$、1 这两种情况。于是，(2.2) 变为

$$F_{11}(r,s) := rs^3 - 3rs^2 - r^2 + 4rs - s = 0,$$

这是 $X_1(11)$ 的一个方程，称为 $X_1(11)$ 的原始形式。通过坐标变换 $r = 1 + xy$ 和 $s = 1 - x$，我们得到

$$f_{11}(x,y) := y^2 + (x^2+1)y + x = 0.$$

这解决了 $X_1(11)$ 的模问题。若我们选取 $x_0 = -1$，并令 $y_0 = -1 + \sqrt{2}$，那么 (x_0, y_0) 是 $X_1(11)$ 上一个 K-有理点，满足 $f_{11}(x_0, y_0) = 0$，其中 $K = \mathbb{Q}(\sqrt{2})$ 是一个

二次数域。若我们将 $x = x_0$ 和 $y = y_0$ 代入 [Su 的表 7] 及公式 (2.1)，便得到

$$\begin{aligned} b_0 := b(x_0, y_0) =& 8 - 6\sqrt{2}, \\ c_0 := c(x_0, y_0) =& 2 - 2\sqrt{2}. \end{aligned}$$

那么，域 K 上的椭圆曲线 $E(b_0, c_0)$ 含有一个阶为 11 的点 (0,0)，事实上，其挠子群为 $\mathbb{Z}/11\mathbb{Z}$。

由 [Su]，可得 [Su 中 $X_1(N)$ 的定义方程，见表 6]；以及 [Su 中将 $X_1(N)$ 从 $f_N(x, y) = 0$ 映至 $F_N(r, s) = 0$ 的双有理映射，见表 7]。其中，$F_N(r, s) = 0$表示 $X_1(N)$ 的原始形式。

现在我们介绍另一种方法，用以解决 Baaziz[B] 引入的 $X_1(N)$ 的模问题。令 $\mathbb{H}$ 为复上半平面，且 $\mathbb{H}^* = \mathbb{H} \cup \mathbb{P}^1(\mathbb{Q})$。那么，$\Gamma_1(N)$ 通过线性分式变换作用于 $\mathbb{H}^*$，而 $X_1(N)(\mathbb{C})$ 可视为黎曼曲面 $\Gamma_1(N)\backslash\mathbb{H}^*$。

$\Gamma_1(N)\backslash\mathbb{H}$ 的点与椭圆曲线 E 的等价类一一对应，并且还指定了一个精确阶为 N 的点 P。令 $L_\tau = [\tau, 1]$ 为 $\mathbb{C}$ 中以 τ 和 1 为基的格。那么，$[\tau] \in \Gamma_1(N)\backslash\mathbb{H}$对应于这一对 $\left[\mathbb{C}/L_\tau, \frac{1}{N} + L_\tau\right]$。因此，$\Gamma_1(N)\backslash\mathbb{H}$ 是一个模空间，用于解决如下模问题：确定有序对（E，P）的等价类，其中 E 是定义在 $\mathbb{C}$ 上的椭圆曲线，$P \in E$ 是一个精确阶为N的点。若存在同构 $E \simeq E'$ 将P 映到 P'，则有序对（E，P）与（E'，P'）等价。

注意，

$$\begin{aligned} &\left[\mathbb{C}/L_\tau,\ \frac{1}{N} + L_\tau\right] \\ &= [y^2 = 4x^3 - g_2(\tau)x - g_3(\tau), (\wp(\frac{1}{N}, \tau), \wp'(\frac{1}{N}, \tau))] \\ &= \left[y^2 + (1 - c(\tau))xy - b(\tau)y = x^3 - b(\tau)x^2,\ (0, 0)\right], \end{aligned} \tag{2.3}$$

其中 $g_2(\tau) = 60G_4(\tau)$，$g_3(\tau) = 140G_6(\tau)$，这里 $G_{2k}(\tau)$ 是权为 $2k$ 的艾森斯坦级数，$\wp(z, \tau) := \wp(z, L_\tau)$ 是魏尔斯特拉斯椭圆函数，而 $b(\tau)$、$c(\tau)$ 是 $\left[\mathbb{C}/L_\tau, \frac{1}{N} + L_\tau\right]$ 中所含 Tate 正规形的系数。此外，若令

$$a(\tau) = \frac{1}{12}\left\{(1 - c(\tau))^2 - 4b(\tau)\right\},$$

于是我们得到以下关系：

$$\begin{aligned} g_2(\tau) =& 12a(\tau)^2 + 2b(\tau)(1 - c(\tau)) \\ g_3(\tau) =& -8a(\tau)^3 - 2a(\tau)b(\tau)(1 - c(\tau)) - b(\tau)^2, \end{aligned}$$

这就得到了（2.3）的最后一个等式（更多详情请参见 [B] ）。

注意到，每个对（E，P）的等价类都包含唯一的 Tate 正规形 [B，命题 1.3],因此，b（τ）和 c（τ）在 Γ_1（N）$\backslash\mathbb{H}$ 上诱导出定义良好的函数。由 [B],

可知

$$b(\tau) = -\frac{(\wp(\frac{1}{N},\tau) - \wp(\frac{2}{N},\tau))^3}{\wp'(\frac{1}{N},\tau)^2}, \tag{2.4}$$

$$c(\tau) = -\frac{\wp'(\frac{2}{N},\tau)}{\wp'(\frac{1}{N},\tau)}$$

是 $\Gamma_1(N)$ 上的模函数，并生成 $X_1(N)$ 的函数域，其中 $\wp'$ 是关于 z 的导数。因此，对于每个非尖点 $\tau \in X_1(N)$，对应一个具有 N-挠点 (0, 0) 的椭圆曲线$E(b(\tau)\ c(\tau))$。

最后，我们描述 $X_\Delta(N)$ 的一些自同构。注意， $X_\Delta(N) \to X_0(N)$ 是一个伽罗瓦覆盖，其伽罗瓦群为 $\Gamma_0(N)/\Gamma_\Delta(N)$，该群同构于 $(\mathbb{Z}/N\mathbb{Z})^*/\Delta$。对于一个与 N 互素的整数a ，令 $[a]$ 表示由 $\gamma \in \Gamma_0(N)$ 表示的 $X_\Delta(N)$ 的自同构，使得$\gamma \equiv \left(\begin{smallmatrix} a & * \\ 0 & * \end{smallmatrix}\right)$ 模 N.。有时我们将 $[a]$ 视为一个矩阵。

对于每个满足 $d|N$with $(d, N/d) = 1$的因子，考虑形如 $\begin{pmatrix} dx & y \\ Nz & dw \end{pmatrix}$ with$x, y, z, w \in \mathbb{Z}$ 且行列式为 d. 的矩阵。这些矩阵定义了 $X_0(N)$ 上唯一的 involution，称为 Atkin-Lehner involution，记作 W_d。特别地，若 $d = N$，则W_N 称为弗里克 involution。我们也用 W_d 表示上述形式的一个矩阵。

如果固定一个矩阵 W_d ，那么 W_d 可能不属于 $\mathrm{PSL}_2(\mathbb{R})$ 中 $\Gamma_\Delta(N)$ 的正规化子 $N(\Gamma_\Delta(N))$，因此可能无法定义 $X_\Delta(N)$ 的自同构。不过， W_d 总是包含于 $N(\Gamma_1(N))$ 中；因此它定义了 $X_1(N)$ 的一个自同构。但它可能无法定义 $X_1(N)$ 的一个 involution。例如， $W_2 = \begin{pmatrix} 2 & 1 \\ 26 & 14 \end{pmatrix}$ 定义了 $X_1(26)$ 的一个 8 阶自同构。此外，若 a 遍历 $(\mathbb{Z}/N\mathbb{Z})^*/\Delta$，则 $[a]W_d$ 给出了 $X_\Delta(N)$ 的不同自同构；这些自同构在 $X_0(N)$ 上诱导相同的 Atkin-Lehner involution W_d。

对于无平方因子 N，Momose 在其未发表的著作 [Mo] 中声称，自同构群 $\mathrm{Aut}(X_\Delta(N))$ 等于$N(\Gamma_\Delta(N))/\Gamma_\Delta(N)$。但是，作者、Kim 和 Schweizer [JKS2] 为 $X_\Delta(37)$ 的情形找到了一个反例，其中 $\Delta = \{\pm1, \pm6, \pm8, \pm10, \pm11, \pm14\}$。因此，可以得出结论：即使对于无平方因子 N， $X_1(N)$ 的自同构群也尚未完全确定。

3. Non-tetraelliptic curves

为确定非四椭圆曲线 $X_1(N)$，我们首先列出如下有理曲线、椭圆曲线、双椭圆曲线或三椭圆曲线 $X_1(N)$:

定理 3.1。([JK，J]) 以下结论成立：

(1) $X_1(N)$ 是有理的，当且仅当 $N = 1 - 10$，12。(2) $X_1(N)$ 是椭圆的，当且仅当 $N = 11$，14，15。(3) $X_1(N)$ 是双椭圆的，当且仅当 $N = 13$，16，17，18，20，21，22，24。(4) $X_1(N)$ 在 $\mathbb{Q}$ 上是三椭圆的，当且仅当 $N = 19$，21，22，27，30

设 X 是域 K 上的一条光滑射影曲线。 X 的 K-丢番图映射度 $\mathrm{Gon}_K(X)$ 是有限 K-有理映射 $X \to \mathbb{P}^1$ 的最小次数。

命题 3.2. ([A], [Ki]) 设 $\Gamma \subseteq \mathrm{SL}_2(\mathbb{Z})$ 为一个同余子群。模曲线 $X(\Gamma)$ 的 $\mathbb{C}$-丢番图映射度至少为 $\frac{\lambda_1}{24}[\mathrm{SL}_2(\mathbb{Z}) : \Gamma]$，其中 $\lambda_1 \geq \frac{975}{4096}$。

假设 X 是四椭圆的，并且存在一个 $\mathbb{Q}$-有理四椭圆映射 $X \to E$，其对应某条椭圆曲线 E。由于存在一个次数为 2 的 $\mathbb{Q}$-有理映射 $E \to \mathbb{P}^1$，$\mathrm{Gon}_{\mathbb{Q}}(X) \leq 8$。由于 $\mathrm{Gon}_{\mathbb{C}}(X) \leq \mathrm{Gon}_{\mathbb{Q}}(X)$，应用命题 3.2，可得：

Lem命题 3.3. $X_1(N)$ 在 $\mathbb{Q}$ 上对于 $N = 41$、43、45、47 和 $N \geq 4$ 不是四椭圆的 9.

证明。注意到 $[\mathrm{SL}_2(\mathbb{Z}) : \Gamma] = \varphi(N)\psi(N)2$，其中 $\psi(N) = N \prod_{p|N}\left(1+\frac{1}{p}\right)$。根据命题$_{p:\ prime}$

3.2，$\mathrm{Gon}_{\mathbb{C}}(X_1(N)) \geq \frac{325\varphi(N)\psi(N)}{65536}$，由不等式即可得到结论

$$\frac{325\varphi(N)\psi(N)}{65536} > 8.$$

□

另一方面，Derickx 和 van Hoeij [DH，表 1] 计算了 $N \leq 40$ 的 $\mathrm{Gon}_{\mathbb{Q}}(X_1(N))$，并给出了 $N \leq 250$ 的上界。以下结果来自该表。

引理 3.4. $X_1(N)$ 在 $\mathbb{Q}$ 上对于 $N = 29$、31、$33-35$、$37-40$、42、44、46、48 不是四椭圆的。

根据引理 3.4，除$N = 42$、44、46 和 48 外，$\mathrm{Gon}_{\mathbb{Q}}(X_1(N)) > 8$ 在 [DH 的表 1] 中可查到 N；而 $\mathrm{Gon}_{\mathbb{Q}}(X_1(42)) > 8$ 则见于 [DH]第 67 页。

假设存在一条定义在 $\mathbb{Q}$上的四椭圆映射 $X_1(N) \to E$，其对应某条椭圆曲线 E。那么 E 的导子整除 N。结合这一事实与 [C 的表1], ，我们得到：

引理 3.5. 对于 $N = 13$、16、18、22、23、25，$X_1(N)$ 在 $\mathbb{Q}$ 上不是四椭圆的。

我们回顾一个关于模参数化的基本事实。

命题 3.6. [S，(1.4) 命题] 设 $\mathcal{E}$ 是一个定义在 $\mathbb{Q}$上的导子为 N的椭圆曲线同源类。那么存在一条椭圆曲线 E_1 及一个模参数化

$$\pi_1 : X_1(N) \to E_1$$

使得若 $\pi : X_1(N) \to E$ 是椭圆曲线 $E \in \mathcal{E}$的参数化，则存在一个同源映射 $\phi : E_1 \to E$，使下图交换：

$$\begin{array}{ccc} X_1(N) & \xrightarrow{\pi} & E_1 \\ & \searrow^{\pi'} & \downarrow \phi \\ & & E \end{array}$$

命题 3.6 中的椭圆曲线 E_1 称为 $X_1(N)$-最优曲线。另一方面，对于 $X_0(N)$ 的模参数化，存在一条具有命题 3.6 所述相同性质的椭圆曲线 E_0，称为 $X_0(N)$-最优曲线。

引理 3.7。 $X_1(19)$ 和 $X_1(27)$ 在 $\mathbb{Q}$ 上不是四椭圆的。

证明。假设存在一条定义在 $\mathbb{Q}$ 上的有理四椭圆映射 $\phi : X_1(19) \to E$，其目标是某条椭圆曲线 E。那么 E 的导子为 19。根据定理 3.1，$X_1(19)$ 在 $\mathbb{Q}$ 上是三椭圆的，因此存在一条定义在 $\mathbb{Q}$ 上的有理映射 $\phi' : X_1(19) \to E'$，次数为 3，其目标是某条导子为

19 的椭圆曲线。根据 [C，表 1]，，导子为 19 的同源类只有一个，因此 E和 E' 是 $\mathbb{Q}$-同源的。由于 X_1(19) 既不是有理曲线，也不是椭圆曲线或双椭圆曲线， E' 是 X_1(19)-最优的；但由于次数关系， ϕ 无法经由 ϕ' 分解，因此产生矛盾。由此可知， X_1(19) 在 $\mathbb{Q}$ 上不是四椭圆的。

通过完全相同的证明，可以证明 X_1(27) 在 $\mathbb{Q}$ 上不是四椭圆的。 □

引理 3.8. X_1(36) 在 $\mathbb{Q}$ 上不是四椭圆的。

证明。对于导子整除36的椭圆曲线，在 $\mathbb{Q}$ 上只有一个同源类，且该类的导子为36。实际上，它是 X_0(36) 的同源类。现在假设 X_1(36) 在 $\mathbb{Q}$ 上是四椭圆的。根据命题 3.6，该同源类中存在一条椭圆曲线 E，它对于来自 X_1(36) 的一致化而言是最优的。从 X_1(36) 到 E 的映射次数必须整除4（由四椭圆映射可知），同时也必须整除6（由从 X_1(36) 到椭圆曲线 X_0(36) 的次数为6的映射可知）。因此， X_1(36) 将是双椭圆的，这与定理 3.1 矛盾。□

引理 3.9. X_1(21) 在 $\mathbb{Q}$ 上不是四椭圆的。

证明。沿用引理 3.8 的完全相同证明，可以计算得出，若 X_1(21) 在 $\mathbb{Q}$ 上是四椭圆的，则它必定在 $\mathbb{Q}$ 上是双椭圆的。然而，根据 [JK，引理 3.5]， X_1(21) 不存在到椭圆曲线的次数为 2 的 $\mathbb{Q}$-有理映射。□

注记 3.10. X_1(21) 是四椭圆的，但并非在 $\mathbb{Q}$ 上。事实上，存在一个次数为 2 的映射 X_1(21) $\to X_\Delta$(21)，其中 $\Delta = \{\pm 1, \pm 8\}$。根据 [JKS2，表1]，，我们知道 X_Δ(21) 是一条双椭圆曲线，具有双椭圆对合 W_{21}；因此 X_1(21) 是一条四椭圆曲线。注意， W_{21} 在 $\mathbb{Q}$ 上未定义。

4. Tetraelliptic curves over $\mathbb{Q}$

为方便读者，我们将定理 1.1 重述如下： $X_1(N)$ 是 $\mathbb{Q}$ 上的四椭圆曲线，当且仅当 $N = 17$、20、24、26、28、30、32。此外，它们存在 $\mathbb{Q}$ 有理的伽罗瓦映射，例如 ϕ_N，从 $X_1(N)$ 映射到次数为 4 的椭圆曲线。特别是对于 $N = 17$、20、26、30 和 32， $X_1(N)$ 是循环四椭圆的，而其他的不是。

在本节中，对于上述列出的 N，我们证明 $X_1(N)$ 是 $\mathbb{Q}$ 上的四椭圆曲线，并为某些椭圆曲线 E_N 构造四椭圆映射 ϕ_N: $X_1(N) \to E_N$。此外，我们利用 ϕ_{17}，找到了定义在循环四次数域上的挠子群为 $\mathbb{Z}/17\mathbb{Z}$ 的椭圆曲线。

4.1. 定理 1.1 的证明。对于 $N = 17$、20、24、28、32，从 $X_1(N)$ 到椭圆曲线存在自然四椭圆映射，即 ϕ_{17}： X_1(17) $\to X_{\Delta_1}$(17)、 ϕ_{20}： X_1(20) $\to X_0$(20)、ϕ_{24}： X_1(24) $\to X_0$(24)、 ϕ_{28}： X_1(28) $\to X_1$(14)，以及 ϕ_{32}： X_1(32) $\to X_{\Delta_2}$(32)，其中 Δ_1 $=\{\pm 1, \pm 2, \pm 4, \pm 8\}$ 和 $\Delta_2 = \{\pm 1, \pm 7, \pm 9, \pm 15\}$。于是， $G_{17} = \langle [2] \rangle$、 $G_{20} = \langle [3] \rangle$ 和 $G_{32} = \langle [7] \rangle$是 4 阶循环群，而 $G_{24} = \langle [5]$、 $[7] \rangle$ 和 $G_{28} = \langle [13]$、 $\nu \rangle$ 是克莱因四元群，其中$\nu = \begin{pmatrix} 1 & 0 \\ 14 & 1 \end{pmatrix}$。稍后我们将确定 ϕ_N 的每个目标曲线是否与 [Cr] 中标记的某条椭圆曲线相同。

现在考虑剩余的情形，即 X_1(26) 和 X_1(30)。令 $\mathcal{E}$ 表示定义在 $\mathbb{Q}$ 上的导子为 N的椭圆曲线同源类。一般而言， $X_0(N)$-最优曲线 $E_0 \in \mathcal{E}$ 与 $X_1(N)$-最优曲线 $E_1 \in \mathcal{E}$ 并不相同。例如， $E_0 = X_0$(11) 和 $E_1 = X_1$(11) 相差一个 5-同源。Stein 和 Watkins [SW] 对 E_0 与

E_1 相差一个 3-同源的情形提出了一个基于数值观察的精确猜想。Lee [Y] 证明了该猜想的一些部分结果，并给出了一个导子为 26 的同源类实例，其中 $X_0(26)$-最优曲线 26A1 与 $X_1(26)$-最优曲线 26A3 相差一个 3-同源。根据 [Cr], 中的表 5，模参数化 $X_0(26) \to 26$A1 的次数为 2，而自然映射 $X_1(26) \to X_0(26)$ 的次数为 6；因此，它们的复合映射 $X_1(26) \to 26$A1 的次数为 12。根据命题 3.6，该映射可经由模参数化 $X_1(26) \to 26$A3 分解；26A3 与 26A1 相差一个 3-同源，因此 $X_1(26) \to 26$A3 的次数必为 4。因此， $X_1(26)$ 是定义在 $\mathbb{Q}$上的四椭圆曲线。

现在我们来求四椭圆映射 $\phi_{26}: X_1(26) \to 26$A3。Bars [B] 证明了$X_0(26)$ 是一条双椭圆曲线，而 W_2 和 W_{13} 是它的全部双椭圆对合。根据 LMFDB [LM], , 26A1 的权 2 对应尖点形式 f 的第二个傅里叶系数为 -1 ，因此 f 在 W_2 下的特征值为 $+1$；于是商空间 $X_0(26)/W_2$ 等于 26A1。供参考， $X_0(26)/W_{13}$ 等于 26B1。那么，26A1 应为 $X_1(26)/G$，其中 G 是由 $Gal(X_1(26)/X_0(26)) = \langle [7] \rangle$ 和 W_2生成的 12 阶群。由于 W_2作为 $X_1(26)$ 的自同构具有 12 阶，群 $G = \langle W_2 \rangle$ 是循环的。现在， ϕ_{26} 是一个伽罗瓦映射，其伽罗瓦群是 G 的一个 4 阶子群。由于 G 只有一个 4 阶子群 $\langle W_2^3 \rangle$，四椭圆映射 ϕ_{26} 应当是一个伽罗瓦群为 $\langle W_2^3 \rangle$的循环映射。

接下来考虑 $X_1(30)$ 的情形。假设存在一条 $\mathbb{Q}$-有理的四椭圆映射 $\phi: X_1(30) \to E$ ，其目标为某条椭圆曲线 E。那么 E 的导子为 15 或 30。若 E 的导子为 30，则根据定理 3.1，E 是 $X_1(30)$-最优曲线。同源类 E 中的 $X_0(30)$-最优曲线是 30A1。由 [B] 可知， $X_0(30)$ 恰有 3 个双椭圆对合，分别是 W_5、W_6 和 W_{30}。用与 $X_1(26)$ 相同的方法可以验证， $X_1(30)/W_5$ 等于 30A1。令 F 为 $X_0(30)$ 与 E 的函数域的复合域，它包含于 $X_1(30)$ 的函数域中。但由于 $X_1(30)$ 是 $X_0(30)$ 的 4 次循环扩张，因此只有一个中间域。所以， F 必定是 $X_\Delta(30)$ 的函数域，其中 $\Delta = \{\pm 1, \pm 11\}$。这意味着映射 ϕ 可经由 $X_\Delta(30)$ 分解。因此， ϕ 必由由 $Gal(X_1(30)/X_0(30)) = \langle [7] \rangle$ 和 W_5 生成的 8 阶群的某个 4 阶子群给出。由于 G 是二面体群，它有 3 个 4 阶子群。采用我们稍后将介绍的方法，我们计算了 $X_1(30)$ 对每个 4 阶子群的商空间，但没有一种情形下得到的商空间是定义在 $\mathbb{Q}$ 上的椭圆曲线，这就产生了矛盾。

因此 E 应当具有导子 15。然而，这种情况很难处理，而且已知结果不多。因此，我们尝试计算 $\mathrm{Aut}(X_1(30))$ 的 4 阶子群所对应的商空间，最终得到了所需结果。考虑由 $[7]$ 和 W_6 生成的 8 阶子群，它是一个二面体群，并令 $H = \langle [11], [7]W_6 \rangle$ 为一个克莱因四元子群。那么商空间 $X_1(30)/H$ 等于 15A8，因此 $\phi_{30}: X_1(30) \to 15$A8 是一个 $\mathbb{Q}$-有理的四椭圆映射，并且 $X_1(30)$ 在 $\mathbb{Q}$上是四椭圆的。

总结以上所有结果，我们完成定理 1.1 的证明。

4.2. 四椭圆映射的构造。从现在起，我们将显式构造四椭圆映射 $\phi_N: X_1(N) \to E_N$ ，即根据第 2 节中介绍的定义方程 $f_N(x, y) = 0$，求出 $X_1(N)$的 ϕ_N 关于 x 和 y 的有理表达式。

首先考虑 $X_1(17)$ 的情形。然后，映射 $X_1(17) \to X_{\Delta_1}(17) = X_1(17)/\langle [2] \rangle$ 是一个如上所述的四椭圆映射。如果我们取 $[2] = (2\ 117\ 9)$，那么 $[2]$ 在 $X_1(17)$ 上的作用为

$[2]\tau = \frac{2\tau+1}{17\tau+9}$。在这种情况下，我们有如下结论：

$$\begin{aligned}\wp\left(\frac{1}{17},[2]\tau\right) &= (17\tau+9)^2\wp\left(\frac{17\tau+9}{17},\tau\right)\\ &= (17\tau+9)^2\wp\left(\frac{9}{17},\tau\right),\end{aligned}$$

and

$$\begin{aligned}\wp'\left(\frac{1}{17},[2]\tau\right) &= (17\tau+9)^3\wp'\left(\frac{17\tau+9}{17},\tau\right)\\ &= (17\tau+9)^3\wp'\left(\frac{9}{17},\tau\right).\end{aligned}$$

因此，由 (2.4) 可得：

$$\begin{aligned}b([2]\tau) &= -\frac{\left(\wp\left(\frac{9}{17},\tau\right)-\wp\left(\frac{1}{17},\tau\right)\right)^3}{\wp'\left(\frac{9}{17},\tau\right)^2},\\ c([2]\tau) &= -\frac{\wp'\left(\frac{1}{17},\tau\right)}{\wp'\left(\frac{9}{17},\tau\right)}.\end{aligned} \tag{4.1}$$

类似地，我们有

$$\begin{aligned}b([4]\tau) &= -\frac{\left(\wp\left(-\frac{4}{17},\tau\right)-\wp\left(-\frac{8}{17},\tau\right)\right)^3}{\wp'\left(-\frac{4}{17},\tau\right)^2},\\ c([4]\tau) &= -\frac{\wp'\left(-\frac{8}{17},\tau\right)}{\wp'\left(-\frac{4}{17},\tau\right)},\end{aligned} \tag{4.2}$$

and

$$\begin{aligned}b([8]\tau) &= -\frac{\left(\wp\left(-\frac{2}{17},\tau\right)-\wp\left(-\frac{4}{17},\tau\right)\right)^3}{\wp'\left(-\frac{2}{17},\tau\right)^2},\\ c([8]\tau) &= -\frac{\wp'\left(-\frac{4}{17},\tau\right)}{\wp'\left(-\frac{2}{17},\tau\right)}.\end{aligned} \tag{4.3}$$

由 (2.1) 和 [Su, 表 7], 可知，满足 $f_{17}(x,y)=0$ 的 $X_1(17)$ 的函数域生成元 x,y 可表示为关于 b,c 的如下函数：

$$\begin{aligned}x &= -\frac{(-c^2+b-c)(-c^3+b^2-bc)}{bc^4+c^5-3b^2c^2+3bc^3+b^3-2b^2c+bc^2},\\ y &= -\frac{(-c^2+b-c)(-bc^2+2b^2-3bc+c^2)}{bc^4+c^5-3b^2c^2+3bc^3+b^3-2b^2c+bc^2}.\end{aligned} \tag{4.4}$$

根据 [L 第 46], 页命题3中的公式，我们可以确定 $\wp(z,\tau)$ 和 $\wp'(z,\tau)$ 的 q 展开，其中 $q=e^{2\pi i\tau}$。利用这些 q 展开以及 (2.4)、(4.1) 和 (4.4)，我们得到

以下 q展开式:

$$\begin{aligned}
x(\tau) =& -\phi^{12}-\phi^{11}-\phi^{10}-2\phi^{9}-2\phi^{8}-\phi^{7}-\phi^{6}-\phi^{5}+O(q),\\
y(\tau) =& \phi^{15}-2\phi^{14}-2\phi^{13}+\phi^{12}-\phi^{11}-3\phi^{10}-3\phi^{7}-\phi^{6}\\
&+\phi^{5}-2\phi^{4}-2\phi^{3}+\phi^{2}-3+O(q),\\
x([2]\tau) =& -\phi^{14}-2\phi^{13}-\phi^{12}-\phi^{11}-\phi^{6}-\phi^{5}-2\phi^{4}-\phi^{3}+O(q),\\
y([2]\tau) =& -3\phi^{15}-2\phi^{14}-\phi^{13}-4\phi^{12}-3\phi^{10}-\phi^{9}-\phi^{8}-3\phi^{7}\\
&-4\phi^{5}-\phi^{4}-2\phi^{3}-3\phi^{2}-4+O(q),\\
x([4]\tau) =& -2\phi^{15}-\phi^{14}-\phi^{11}-\phi^{10}-\phi^{7}-\phi^{6}-\phi^{3}-2\phi^{2}+O(q),\\
y([4]\tau) =& 2\phi^{15}+3\phi^{14}+2\phi^{13}-\phi^{11}+\phi^{10}+3\phi^{9}+3\phi^{8}+\phi^{7}\\
&-\phi^{6}+2\phi^{4}+3\phi^{3}+2\phi^{2}-1+O(q),\\
x([8]\tau) =& 2\phi^{15}+\phi^{14}+2\phi^{13}+\phi^{12}+2\phi^{11}+\phi^{10}+2\phi^{9}+2\phi^{8}\\
&+\phi^{7}+2\phi^{6}+\phi^{5}+2\phi^{4}+\phi^{3}+2\phi^{2}+2+O(q),\\
y([8]\tau) =& -3\phi^{14}+\phi^{13}-\phi^{12}-2\phi^{11}+\phi^{10}-2\phi^{9}-2\phi^{8}+\phi^{7}\\
&-2\phi^{6}-\phi^{5}+\phi^{4}-3\phi^{3}-3+O(q),
\end{aligned}$$

其中 ø 是 1 的 21 次本原根。

现在令 $\bar{x}(\tau)=x(\tau)+x([2]\tau)+x([4]\tau)+x([8]\tau)$ 和 $\bar{y}(\tau)=y(\tau)+y([2]\tau)+y([4]\tau)+y([8]\tau)$，于是 $\bar{x},\bar{y}$ 生成 $X_{\Delta_1}(17)$ 的函数域。利用它们，我们可以通过以下算法得到 $X_{\Delta_1}(17)$ 的定义方程。

算法 4.1。(1) 设多项式 $f(x,y)=\sum a_n x^i y^j$，其中 d 是正整数，且$i+j\le d$

未知 a_n。
(2) 输入 $f(x,y)$ 中 $\bar{x}(\tau)$ 和 $\bar{y}(\tau)$ 的 q-展开。(3) 对于方程 $g(\bar{x},\bar{y})=0$，比较 $0\le m\le \frac{(d+1)(d+2)}{2}$ 的 q^m 系数，并建立一个线性方程组。(4) 求解 (3) 中的方程组，得到~~一个定义~~方程。

使用算法 4.1，我们得到 $X_{\Delta_1}(17)$ 的定义方程如下：

$$\begin{aligned}
f(x,y) =& -x^3y^2+x^4-4x^3y-4x^2y^2-4x^3-16x^2y-10xy^2\\
&-y^3-14x^2-46xy-17y^2-60x-70y-100=0.
\end{aligned}$$

使用计算机代数系统 Maple，我们可以将 $g(x,y)$ 转换为魏尔斯特拉斯方程，结果如下:

$$E_{17}: v^2+uv+v=u^3-u^2-6u-4.$$

因此， E_{17} 等于 17A2，其挠群为 $\mathbb{Z}/4\mathbb{Z}$。这里， $X_{\Delta_1}(17)$ 与 E_{17} 之间的一个同构由下式给出：

$$
\begin{aligned}
u(x,y) =&(x^5+x^4y+7x^4+5x^3y+26x^3+15x^2y+xy^2+63x^2+27xy+y^2\\
&+90x+17y+50)/(x^4+4x^3+12x^2+18x+10)\\
v(x,y) =&(x^5y+3x^5+7x^4y+16x^4+25x^3y+x^2y^2+56x^3+58x^2y+3xy^2\\
&+121x^2+73xy+3y^2+136x+41y+70)/(x^4+4x^3+12x^2+18x+10)
\end{aligned}
\tag{4.5}
$$

注 4.2. 采用与上文完全相同的方法，我们可以找到 $N=20$ 对应的目标椭圆曲线 E_N，24，28，32 分别为 20A1、24A1、14A4、32A2。

我们利用 (4.5) 以及 $\bar{x}(\tau)$ 和 $\bar{y}(\tau)$ 的 q-展开，计算函数域 E_{17} 的两个生成元 $u(\tau)$ 和 $v(\tau)$ 的 q-展开，如下：

$$
\begin{aligned}
u(\tau) =& -2\text{ø}^{14}-2\text{ø}^{12}-2\text{ø}^{11}-2\text{ø}^{10}-2\text{ø}^{7}-2\text{ø}^{6}-2\text{ø}^{5}-2\text{ø}^{3}+2+O(q),\\
v(\tau) =& -3\text{ø}^{14}-3\text{ø}^{12}-3\text{ø}^{11}-3\text{ø}^{10}-3\text{ø}^{7}-3\text{ø}^{6}-3\text{ø}^{5}-3\text{ø}^{3}+5+O(q).
\end{aligned}
$$

现在，我们通过以下算法得到 ϕ_{17} 的显式表达式： $X_1(17)\to E_{17}$。

算法 4.3. (1) 设两个多项式 $g(x,y)=\sum_{i+j\le d} a_n x^i y^j$ 和 $h(x,y)=\sum_{i+j\le d} b_n x^i y^j$ 对于一个正整数 d 以及未知量 a_n 和 b_n。

(2) 输入 $g(x,y)$ 和 $h(x,y)$ 中 $x(\tau)$ 与 $y(\tau)$ 的 q-展开。(3) 对于两个方程 $g(x(\tau)\ y(\tau))=u(\tau)h(x(\tau)\ y(\tau))$ 和 $g(x(\tau)\ y(\tau))=v(\tau)h(x(\tau)\ y(\tau))$，比较 q^m for $0\le m\le (d+1)(d+2)$ 的系数，并建立两个线性方程组。(4) 解出(3)中的方程组后，我们得到一个有理映射 $\begin{pmatrix} g_1(x,y) & g_2(x,y) \\ h_1(x,y) & h_2(x,y)\end{pmatrix}$，其中 $g_1(x,y)$ 和 $h_1(x,y)$（分别为 $g_2(x,y)$ 和 $h_2(x,y)$）通过~~求解由 $g(x(\tau)\ y(\tau))=u(\tau)h(x(\tau)\ y(\tau))$~~（分别由 $g(x(\tau)\ y(\tau))=v(\tau)h(x(\tau)\ y(\tau))$）得到的线性方程组求得。

最后，利用算法 4.3，我们得到四椭圆映射ϕ_{17}的显式表达式： $X_1(17)\to E_{17}$，即 $\phi_{17}(x,y)=(p_1(x,y)\ p_2(x,y))$，如下所示：

$$
\begin{aligned}
p_1(x,y) =&\frac{x^2+xy-y^2+x-2y-1}{(y+1)^2},\\
p_2(x,y) =&\frac{x^3y^2-x^4+2x^3y+2x^2y^2-x^3+x^2y+y^3-xy+y^2}{(y+1)^2(x-y)}.
\end{aligned}
$$

接下来我们将构造四椭圆映射 ϕ_{26}： $X_1(26)\to X_1(26)/\langle W_2^3\rangle = 26\text{A}3$。若取$W_2=\begin{pmatrix}2 & 1\\ 26 & 14\end{pmatrix}$，则 W_2 在 $X_1(26)$ 上的作用为 $W_2\tau=\frac{2\tau+1}{26\tau+14}$。在这种情况下，我们有如下结果：

$$
\begin{aligned}
\wp\left(\frac{1}{26}, W_2\tau\right) &= (26\tau+14)^2\wp\left(\frac{26\tau+14}{26}, 2\tau\right)\\
&= (26\tau+14)^2\wp\left(\tau+\frac{14}{26}, 2\tau\right),
\end{aligned}
$$

and

$$\wp'\left(\frac{1}{26}, W_2\tau\right) = (26\tau+14)^3\wp'\left(\frac{26\tau+14}{26}, 2\tau\right)$$
$$= (26\tau+14)^3\wp'\left(\tau+\frac{14}{26}, \tau\right).$$

因此，由 (2.4) 可得:

$$b(W_2\tau) = -\frac{\left(\wp\left(\tau+\frac{14}{26}, 2\tau\right)-\wp\left(\frac{2}{26}, 2\tau\right)\right)^3}{\wp'\left(\tau+\frac{14}{26}, 2\tau\right)^2}, \tag{4.6}$$
$$c(W_2\tau) = -\frac{\wp'\left(\frac{2}{26}, 2\tau\right)}{\wp'\left(\tau+\frac{2}{26}, 2\tau\right)}.$$

利用这一作用以及与 $X_1(17)$ 情形中完全相同的方法，我们可以找到 ϕ_{26} 的显式表达式，如表1所示。其他情形也可以采用完全相同的步骤处理。我们在表1中列出了定理 1.1 中 N 列表所对应的 ϕ_N 的显式表达式。

表1： ϕ_N的显式表达式

N	$\phi_N = (p_1(x,y)\ p_2(x,y))$的显式表达式
17	$p_1(x,y) = \frac{x^2+xy-y^2+x-2y-1}{(y+1)^2}$, $p_2(x,y) = \frac{x^3y^2-x^4+2x^3y+2x^2y^2-x^3+x^2y+y^3-xy+y^2}{(y+1)^2(x-y)}$
20	$p_1(x,y) = \frac{x^3y-2x^2y+2xy+y^2+2y+2}{(y+1)(x-1)}$, $p_2(x,y) = -\frac{2x^3y^2-xy^4-2x^2y^2+2xy^3+3y^4-2x^2y+4xy^2+7y^3+4xy+8y^2+2x+4y}{2}$
24	$p_1(x,y) = \frac{2x(-xy^2+x^2+xy-2y^2+2y)}{(y+1)(x+y)}$, $p_2(x,y) = \frac{4(x+1)(-x^2y^2+x^3+x^2y-2xy^2+2xy+2y^2)}{-x^2y^2+x^3+x^2y-2xy^2+2xy+2y^2}$
26	$p_1(x,y) = \frac{(y-1)(x^2+x+y)(x+y)}{x^4+x^3y+2x^3+2x^2y+xy^2+x^2-xy-y^2+x+y}$, $p_2(x,y) = -\frac{(y-1)(2xy+y^2-x-y)}{x^4+x^3y+2x^3+2x^2y+xy^2+x^2-xy-y^2+x+y}$
28	$p_1(x,y) = -\frac{x^2(y-1)(x+y)(x+1-y)}{x^4y+4x^3y-2x^3+5x^2y+2xy^2+y^3-3x^2+xy-x}$, $p_2(x,y) = -\frac{y(x+1)(-y^3+x^2-xy+x)}{x^2(xy^2-xy+2y^2+x-2y+1)}$
30	$p_1(x,y) = -\frac{y(x^3y+x^2y+x^2-y^2+x+y)}{x^3y^3+2x^2y^3-x^2y^2-y^4+x^2y+2xy^2+2y^3-2xy-2y^2+x+y}$, $p_2(x,y) = -y(2x^4y^2-x^4y+4x^3y^2+2x^2y^2-2xy^3-x^3+3x^2y+4xy^2-y^3-2x^2-xy+y^2)/$ $(x^5y^2+x^4y^3+x^3y^4+3x^4y^2+2x^3y^3+2x^2y^4+2x^4y+2x^3y^2-2x^2y^3-xy^4-y^5$ $+6x^3y+6x^2y^2+3xy^3+2y^4+x^3-4xy^2-3y^3+3x^2+4xy+2y^2-x-y)$

32	$p_1(x,y)$ =	$-(x-1)(x+1-y)(x^2y^2-xy^3-2x^2y+2xy^2-y+1)/(x^4y^2-2x^3y^3+x^2y^4-2x^3y^2$ $+3x^2y^3-xy^4+2x^3y-x^2y^2-xy^3-3x^2y+3xy^2+x^2-xy+y^2-2y+1)$,
	$p_2(x,y)$ =	$2(x^7y^2-4x^6y^3+6x^5y^4-4x^4y^5+x^3y^6+x^7y-8x^5y^3+12x^4y^4-5x^3y^5-x^6y+6x^5y^2$ $-8x^4y^3+4x^2y^5-xy^6+3x^4y^2-2x^3y^3-5x^2y^4+4xy^5-x^5+x^4y-x^3y^2+13x^2y^3$ $-13xy^4+y^5-x^4+4x^3y-16x^2y^2+18xy^3-4y^4-2x^3+7x^2y-12xy^2+8y^3-x^2$ $+4xy-8y^2+3y)/(3x^7y^2-8x^6y^3+5x^5y^4+2x^4y^5-2x^3y^6-2x^7y+6x^6y^2-8x^5y^3$ $+8x^4y^4-6x^3y^5+2x^2y^6-2x^6y+11x^5y^2-12x^4y^3-x^3y^4+4x^2y^5-5x^5y+5x^4y^2$ $+3x^3y^3-x^2y^4-2xy^5+x^5-3x^4y+5x^3y^2+x^2y^3-4xy^4+2x^4-7x^3y-5x^2y^2$ $+10xy^3+3x^3-x^2y-3xy^2+2y^3+2x^2-2xy-4y^2+x+2y)$

4.3. 椭圆曲线的构造。本小节将构造与 E_{17} 的 $\mathbb{Q}$-有理挠点上方的 $X_1(17)$ 的四次点相对应的椭圆曲线。

注意， $\phi_{17}: X_1(17) \to E_{17}$ 是 4 次循环扩张，且 E_{17} 的挠子群为 $\mathbb{Z}/4\mathbb{Z}$。令$P_1 := (3,-2)$ 和 $P_2 := (-5/4, 1/8)$，它们是E_{17}四个 4 挠点中的两个非零点。对于 P_1，通过求解方程组

$$p_1(x,y) = 3,\ p_2(x,y) = -2,\ f_{17}(x,y) = 0,$$

我们得到位于 P_1 上方的 $X_1(17)$ 的四个点，它们是

$$\left(\alpha_i, \frac{\alpha_i^2}{2} - \frac{\alpha_i}{2} - 2\right) \tag{4.7}$$

其中 α_i 是当 $i = 1$ 取 2、3、4 时 $2x^4 - 5x^3 - 7x^2 + 10x + 8$ 的四个根。对于所有 i，四次数域 $\mathbb{Q}(\alpha_i)$ 都是 $\mathbb{Q}$ 上的循环扩张。同样，我们得到位于 P_2 上方的四个点，它们是

$$(\beta_i, -2\beta_i - 1) \tag{4.8}$$

其中， β_i 是 $8x^4 + 14x^3 - 11x^2 - 11x - 2$ 的四个根， $i = 1$ 为 2、3、4。对于所有 i ，四次数域 $\mathbb{Q}(\beta_i)$ 也都是 $\mathbb{Q}$ 上的循环扩张。我们注意到，$(-1, 0)$ 是 $X_1(17)$ 上位于 E_{17} 的第三个非零点上方的点，并且它是 $X_1(17)$ 的一个尖点；因此我们无法得到相应的椭圆曲线。

由 (2.1) 和 [Su], 的表7可知，与 (4.7) 对应的椭圆曲线为

$$E_{1i} := E\left(-\frac{1337}{32}\alpha_i^3 + \frac{3233}{64}\alpha_i^2 + \frac{12285}{64}\alpha_i + \frac{1135}{16}, -\frac{59}{16}\alpha_i^3 + \frac{147}{32}\alpha_i^2 + \frac{535}{32}\alpha_i + \frac{45}{8}\right), \tag{4.9}$$

与（4.7）对应的椭圆曲线为

$$E_{2i} := E\left(-\frac{6901}{1024}\beta_i^3 - \frac{41387}{4096}\beta_i^2 + \frac{91011}{8192}\beta_i + \frac{39449}{8192}, -\frac{139}{16}\beta_i^3 - \frac{725}{64}\beta_i^2 + \frac{2301}{128}\beta_i + \frac{871}{128}\right). \tag{4.10}$$

那么 E_{1i}（分别为 E_{2i}）是定义在循环四次扩张 $\mathbb{Q}(\alpha_i)$（分别为 $\mathbb{Q}(\beta_i)$）上的椭圆曲线，其底域为 $\mathbb{Q}$，对所有 i，其挠子群为 $\mathbb{Z}/17\mathbb{Z}$ 。

我们在所有其他情形中都尝试了相同的方法，但遗憾的是，未能取得与 17 相同的结果。在所有其他情形中， $X_1(N)$ 上位于挠点上方的点都是尖点，因此无法得到相应的椭圆曲线。

Acknowledgements

我们感谢 Andreas Schweizer 与我们讨论本文中的各种结果。

References

[A] D. Abramovich, *A linear lower bound on the gonality of modular curves*, 《国际数学研究通知》20 (1996), 1005–1011. [B] H. Baaziz, *Equations for the modular curve $X_1(N)$ and models of elliptic curves with torsion points*, 《数学计算》 79 (2010), 第 272 期 , 2371–2386. [C] M. Chou, *Torsion of rational elliptic curves over quartic Galois number fields*, 《数论杂志》160 (2016), 603–628. [Cr] J. E. Cremona, *Algorithms for modular elliptic curves*, 第二版，剑桥大学出版社，剑桥，1997年。[DE] M. Derickx, A. Etropolski, M. van Hoeij, J. S. Morrow, D. Zureick-Brown, *Sporadic cubic torsion*, 《代数与数论》15 (2021), 第7期, 1837–1864. [DH] M. Derickx and M. van Hoeij, *Gonality of the modular curve $X_1(N)$*, 《代数杂志》417 (2014), 52–71. [H] D. Husem¨oller, *Elliptic curves.* 第二版。附录由 Otto Forster、Ruth Lawrence 和 Stefan Theisen 撰写。《数学研究生教材》第 111 卷。施普林格出版社，纽约，2004 年。xxii+487 页。[J] D. Jeon, *Trielliptic modular curves $X_1(N)$*。《算术学报》206 (2022), 171–188. [JK] D. Jeon and C. H. Kim, *Bielliptic modular curves $X_1(N)$*, 《算术学报》112 (2004), 第1期, 75–86. [JKP] D. Jeon, C. H. Kim, and E. Park, *On the torsion of elliptic curves over quartic number fields*, 《伦敦数学会杂志》(2) 74 (2006), 第1期, 1–12. [JKS 1] D. Jeon, C. H. Kim and A. Schweizer, *On the torsion of elliptic curves over cubic number fields*, 《算术学报》113 (2004) 291–301. [JKS2] D. Jeon, C. H. Kim and A. Schweizer, *Bielliptic intermediate modular curves*, 《纯粹与应用代数》224 (2020), 第1期, 272–299. [K] S. Kamienny, *Torsion points on elliptic curves and q-coefficients of modular forms*, 《数学发明》109 (1992) 221–229. [KM] M. A. Kenku and F. Momose, *Torsion points on elliptic curves defined over quadratic fields*, 《名古屋数学杂志》109 (1988), 125–149. [Ki] H. Kim, *Functoriality for the exterior square of GL_4 and the symmetric fourth of GL_2*, 附录1由 D. Ramakrishnan 撰写，附录2由 H. Kim 和 P. Sarnak 撰写，《美国数学会杂志》16 (2003), 139–183. [L] S. Lang, *Elliptic functions*, 第2版。《数学研究生教材》第112卷，施普林格出版社，纽约，1987年。[Le] S. Lang, *Elliptic functions*, 第2版。《数学研究生教材》第112卷，施普林格出版社，纽约，1987年。[LM] LMFDB 协作组, *The L-functions and modular forms database* 2023, , [5 2023] https://www.lmfdb.org, 在线；访问于 5 月。[M] B. Mazur, *Modular curves and the Eisenstein ideal*, 高等科学研究所数学出版物47 (1977), 33–186.[Mo] F. Momose, *Automorphism groups of the modular curves $X_1(N)$*, 未发表的预印本。[N] F. Najman, *Torsion of rational elliptic curves over cubic fields and sporadic points on $X_1(n)$*, 《数学研究快报》23 (2016) 245–272. [S] G. Stevens, *Stickelberger elements and modular parametrizations of elliptic curves*, 《数学发明》98 (1989), 第1期, 75–106. [SW] W. Stein and M. Watkins, *A database of elliptic curves-first report* 载于：《算法数论》（悉尼, 2002 267 275, 2369, 2002 ）—计算机科学讲义。施普林格出版社，柏林，[ ] *Constructing elliptic curves over finite fields with prescribed torsion* Su A. V. Sutherland, , 《数学计算》81 (2012), 1131–1147. [W] J. Wang, *On the torsion structure of elliptic curves over cubic number fields*, 博士论文，2015年。南加州大学。[Y] D. Yhee, *Rational torsion on optimal curves and rank 1 elliptic curves*, 博士论文，2012年。首尔国立大学。

Department of Mathematics Education, Kongju National University, Gongju, 32588 South Ko-rea*Email address*: dyjeon@kongju.ac.kr