arXiv:2301.01680v1 [math.NT] 3 Jan 2023

具有复乘且 2-adic 群垂直纠缠的椭圆曲线

NATHAN JONES

Abstract. 考虑由魏尔斯特拉斯方程 $y^2 = x^3 - 11x - 14$给出的椭圆曲线 E，它具有 $\mathbb{Z}[i]$中导子为 2 的序所给出的复乘。Daniels 和 Lozano-Robledo 最近在一篇论文中指出，对于每个 $n \geq 2$, $\mathbb{Q}(\mu_{2^{n+1}}) \subseteq \mathbb{Q}(E[2^n])$。在本文中，我们证明，这个（先验看来令人惊讶的）“垂直纠缠塔”实际上与其说是一个问题，不如说是一种特征：对于任何具有偶判别式的序所给出复乘的 *any* 椭圆曲线 E（定义在 $\mathbb{Q}$上），这一结论都成立。

1. Main result and proof

设 E 是定义在 $\mathbb{Q}$ 上、具有序 $\mathcal{O}_{K,\,f} \subseteq \mathcal{O}_K$ 在虚二次域 K 中导子为 f 的椭圆曲线。由于 E 的每个自同态都定义在 $\mathbb{Q}$ 上，且与 $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ 的作用可交换，因此伽罗瓦表示的像

$$\rho_{E,m} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{Aut}(E[m]) \simeq \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z}),$$

（其定义为令 $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ 作用于 $E[m]$（即 E 的 m-挠子群），并固定其一个 $\mathbb{Z}/m\mathbb{Z}$-基）包含在某个子群 $\mathcal{N}_{\delta,\phi}(m) \subseteq \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$ 中，我们现在仿照 [2] 对其进行说明。首先，设

$$\phi = \phi(\mathcal{O}_{K,f}, m) := \begin{cases} 0 & \text{if } \Delta_K f^2 \equiv 0 \bmod 4 \text{ or if } m \text{ is odd}, \\ f & \text{if } \Delta_K f^2 \equiv 1 \bmod 4 \text{ and } m \text{ is even}, \end{cases}$$

$$\delta = \delta(\mathcal{O}_{K,f}, m) := \begin{cases} \Delta_K f^2/4 & \text{if } \Delta_K f^2 \equiv 0 \bmod 4 \text{ or if } m \text{ is odd}, \\ (\Delta_K - 1)f^2/4 & \text{if } \Delta_K f^2 \equiv 1 \bmod 4 \text{ and } m \text{ is even}. \end{cases}$$

接下来，我们将相应的卡当子群 $\mathcal{C}_{\delta,\phi}(m)$ 定义为

$$\mathcal{C}_{\delta,\phi}(m) := \left\{ \begin{pmatrix} a + b\phi & b \\ b\delta & a \end{pmatrix} : a, b \in \mathbb{Z}/m\mathbb{Z},\, a^2 + \phi ab - \delta b^2 \in (\mathbb{Z}/m\mathbb{Z})^\times \right\}. \tag{1}$$

最后，我们将 $\mathcal{N}_{\delta,\phi}(m) \subseteq \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$ 定义为

$$\mathcal{N}_{\delta,\phi}(m) := \left\langle \begin{pmatrix} -1 & 0 \\ \phi & 1 \end{pmatrix}, \mathcal{C}_{\delta,\phi}(m) \right\rangle. \tag{2}$$

若 E 是定义在 $\mathbb{Q}$ 上、具有 CM（复乘）且由 $\mathcal{O}_{K,f}$ 给出的任意椭圆曲线，则对 $E[m]$ 的适当 $\mathbb{Z}/m\mathbb{Z}$-基，有 $\rho_{E,m}(G_{\mathbb{Q}}) \subseteq \mathcal{N}_{\delta,\phi}(m)$。更多细节请参见 [2]。

令 E_{-16} 为由魏尔斯特拉斯方程 $y^2 = x^3 - 11x - 14$ 定义的椭圆曲线（即 Cremona 标记为 32a3 的椭圆曲线）。曲线 E_{-16} 具有 CM，其对应于域 $\mathbb{Q}(i)$ 中导子为 2 的序 $\mathcal{O} := \mathbb{Z} + 2i\mathbb{Z}$。此外，正如 [1, 定理 1.5], 中所指出的，我们有

$$n \in \mathbb{N}_{\geq 2} \implies \mathbb{Q}(\zeta_{2^{n+1}}) \subseteq \mathbb{Q}(E_{-16}[2^n]). \tag{3}$$

作者还观察到，分别由魏尔斯特拉斯方程 $y^2 = x^2 + x$ 和 $y^2 = x^3 + 2x$ 给出的椭圆曲线 $E_{-4,\,1}$ 和 $E_{-4,\,2}$满足

$$\mathbb{Q}(E_{-4,1}[2]) = \mathbb{Q}(\zeta_4) \quad \text{and} \quad \mathbb{Q}(\zeta_8) \subseteq \mathbb{Q}(E_{-4,2}[4]).$$

本文旨在证明，这两条椭圆曲线 $E_{-4,\,1}$ 和 $E_{-4,\,2}$ 也满足（3）。更一般地，我们将证明以下定理。

定理 1.1. 设 E 是定义在 $\mathbb{Q}$ 上、具有复乘的任意椭圆曲线，其复乘由虚二次域 K 中的一个序 $\mathcal{O}_{K,\,f}$ 给出。假设 $\mathcal{O}_K$ 的判别式 $\Delta_K f^2$，f 为偶数，则对于每个 $n \in \mathbb{N}_{\geq 2}$，有 $\mathbb{Q}(\zeta_{2^{n+1}}) \subseteq \mathbb{Q}(E[2^n])$。

证明. 记 $G(2^n) := \rho_{E,\,2^n}(G_{\mathbb{Q}}) \subseteq \mathcal{N}_{\delta,\,\phi}(2^n)$ 为与 E 相关的模 2^n 像。我们将证明，对于每个 $n \in \mathbb{N}_{\geq 2}$，存在一个满同态 $\delta\colon G(2^n) \twoheadrightarrow (\mathbb{Z}/2^{n+1}\mathbb{Z})^\times$，使得 $\det|_{G(2^{n+1})} = \delta \circ \pi$，其中 $\pi\colon G(2^{n+1}) \to G(2^n)$ 表示投影映射。换言之，下图将交换：

$$\begin{array}{ccc} G(2^{n+1}) & \xrightarrow{\det} & (\mathbb{Z}/2^{n+1}\mathbb{Z})^\times \\ \downarrow{\scriptstyle \pi} & \overset{\delta}{\nearrow} & \downarrow \\ G(2^n) & \xrightarrow{\det} & (\mathbb{Z}/2^n\mathbb{Z})^\times. \end{array} \tag{4}$$

一旦确立这一点，便可推出

$$\mathbb{Q}(\zeta_{2^{n+1}}) = \mathbb{Q}(E[2^{n+1}])^{\ker\det} = \mathbb{Q}(E[2^{n+1}])^{\pi^{-1}(\ker\delta)} = \mathbb{Q}(E[2^n])^{\ker\delta} \subseteq \mathbb{Q}(E[2^n]). \tag{5}$$

关键的观察是，由于假设 $\Delta_K f^2$ 为偶数，因此可得 $\phi = 0$。结合 (1) 和 (2)，我们便可看到

$$n \in \mathbb{N}_{\geq 2} \Longrightarrow \ker\left(\mathcal{N}_{\delta,\,\phi}(2^{n+1}) \to \mathcal{N}_{\delta,\,\phi}(2^n)\right) \subset \mathrm{SL}_2(\mathbb{Z}/2^{n+1}\mathbb{Z}). \tag{6}$$

（我们要求 $n > 1$ 的原因是，否则便无法得到 $\ker(\mathcal{N}_{\delta,\,\phi}(2^{n+1}) \to \mathcal{N}_{\delta,\,\phi}(2^n)) \subseteq \mathcal{C}_{\delta,\,\phi}(2^{n+1})$，因为 $\begin{pmatrix} -1 & 0 \\ \phi & 1 \end{pmatrix} \equiv I$ 对 2 取模；对于 $n = 1$，(6) 的推论不成立。）现在我们定义映射 δ 为

$$\delta(g) := \det(g'), \qquad \text{where } g' \in \pi^{-1}(g).$$

根据 (6)，该映射与 $g' \in \pi^{-1}(g)$ 的选取无关，因此定义了一个映射 $\delta\colon G(2^n) \to (\mathbb{Z}/2^{n+1}\mathbb{Z})^\times$。它是满射，因为 $\det\colon G(2^{n+1}) \to (\mathbb{Z}/2^{n+1}\mathbb{Z})^\times$ 是满射；根据 δ 的定义，图表 (4) 交换。因此，由 (5) 可推得

$$\forall n \in \mathbb{N}_{\geq 2}, \quad \mathbb{Q}(\zeta_{2^{n+1}}) \subseteq \mathbb{Q}(E[2^n]),$$

正如所断言的。 □

定理 1.1 的证明适用于以下更一般的情形。给定一个代数群 $\mathcal{G}$ 和 $\hat{\mathbb{Z}}$ 一个伽罗瓦表示 $\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathcal{G}(\hat{\mathbb{Z}})$，记 $\rho_m : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathcal{G}(\mathbb{Z}/m\mathbb{Z})$ 为 ρ 与自然投影映射 $\mathcal{G}(\hat{\mathbb{Z}}) \to \mathcal{G}(\mathbb{Z}/m\mathbb{Z})$ 的复合，并定义 $\mathbb{Q}(E(\rho[m])) := \overline{\mathbb{Q}}^{\ker\rho_m}$.

定义 1.2. 假设 $\mathcal{G}$ 是一个存在同态 $\delta\colon \mathcal{G} \to \mathbb{G}_m$ 到乘法群的任意代数群。若伽罗瓦表示 $\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathcal{G}(\hat{\mathbb{Z}})$ 满足 $\delta_{\hat{\mathbb{Z}}} \circ \rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathcal{G}(\hat{\mathbb{Z}}) \to \mathbb{Z}^\times$ 与分圆特征一致，则称其延拓了分圆特征。对于任意素数p，若存在 $n_0 \in \mathbb{N}$，使得对每个$n \in \mathbb{N}_{\geq n_0}$，都有 $\ker\left(\mathcal{G}(\mathbb{Z}/p^{n+1}\mathbb{Z}) \to \mathcal{G}(\mathbb{Z}/p^n\mathbb{Z})\right) \subseteq \ker \delta_{p^{n+1}}$，则称 $\mathcal{G}(\mathbb{Z}_p)$ 构成一个垂直纠缠的 p-进群；其中 $\delta_{p^{n+1}}\colon \mathcal{G}(\mathbb{Z}/p^{n+1}\mathbb{Z}) \to (\mathbb{Z}/p^{n+1}\mathbb{Z})^\times$表示与 δ 在 $\mathcal{G}$的 mod p^{n+1} 点上对应的群同态。

注 1.3. 设 $\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathcal{G}(\hat{\mathbb{Z}})$ 是任意一个延拓分圆特征的伽罗瓦表示，并假设对于某个素数 p，群 $\mathcal{G}(\mathbb{Z}_p)$ 是一个垂直纠缠的 p- 进群。那么，定理 1.1 的证明表明，在这一更一般的情形下，我们有

$$\forall n \in \mathbb{N}_{\geq n_0}, \quad \mathbb{Q}(\mu_{p^{n+1}}) \subseteq \mathbb{Q}(\rho[p^n]).$$

2. Acknowledgement

作者谨慎感谢 Harris Daniels 提请他注意这一现象 (3)，并且还感谢 Ken McMurdy 进行了后续富有启发性的讨论。

References

[1] H. Daniels 和 A. Lozano-Robledo, *Coincidences of division fields*, 预印本。即将在 Ann. Inst. Fourier 发表。可通过 https://arxiv.org/abs/1912.05618 获取

[2] A. Lozano-Robledo, *Galois representations attached to elliptic curves with complex multiplication*, 预印本。即将在 Algebra and Number Theory 发表。可通过 https://arxiv.org/abs/1809.02584 获取

Department of Mathematics, Statistics and Computer Science, University of Illinois at Chicago, 851 S Morgan St, 322 SEO, Chicago, 60607, IL, USA *Email address*: ncjones@uic.edu