arXiv:2304.03964v1 [math.NT] 8 Apr 2023

椭圆曲线上的局部非本原点

NATHAN JONES、FRANCESCO PAPPALARDI 和 PETER STEVENHAGEN

Abstract. 在广义黎曼猜想下，数域 K 的乘法群中的任何全局本原元（即在 K^* 中不是完全幂的元）都是某个正密度素数集合模意义下的本原根。

对于已知具有无穷多个 E/K 循环约化素数 $\mathfrak{p}$的椭圆曲线（可能需要广义黎曼猜想），一个全局本原点 $P \in E(K)$ 可能无法生成任何点群 $E(k_\mathfrak{p})$。我们用相关的伽罗瓦表示$\rho_{E/K,\,P} : G_K \to \mathrm{GL}_3(\mathbb{Z})$来描述这一现象，并利用它构造椭圆曲线上的全局点的非平凡例子，这些点是局部非本原的。

1. Introduction

在广义黎曼猜想（GRH）下，每个既非 -1 也非平方的非零有理数，都是无穷多个素数 p模意义下的本原根。这一结果由 Hooley 于 1967年 [5], 证明，时间距 Artin 将其提出为猜想已有四十年。对于一般数域 K，这一陈述的直接类比存在反例，即存在数域 K 含有非挠元 $x \in K^*$，这些元不是 ℓ任意素数 ℓ 次幂，且 K 包含一个本原 ℓ次单位根，但它们在仅有限多个剩余类域中是本原根 $k_\mathfrak{p}$。不过，Artin 猜想的直接类比对于$x \in K^*$ 那些全局本原的 $K^{*\ell}$ （即对于任意素数 ℓ都不属于）仍然成立。

定理 1.1. 设 K 是一个数域，且 $x \in K^*$ 全局本原，并假设广义黎曼猜想成立。则对于正密度的 K 中的一组素数 $\mathfrak{p}$， x 是模 $\mathfrak{p}$ 的本原根。

通俗地说：全局本原的元素 K^* 在无穷多个处 $k_\mathfrak{p}^*$ 都是局部本原的 $\mathfrak{p}$，其中“本原”在 K^* 或 $k_\mathfrak{p}^*$ 中的含义是：它生成的子群不包含在 K^* 或 $k_\mathfrak{p}^*$的严格更大的循环子群中。第3 节证明定理1.1，并给出更强命题的反例。

现在用椭圆曲线 E/K的点群 $E(K)$替换乘法群 K^*，并用 E在良约化素数 $\mathfrak{p}$ 处的剩余类域的单位群 $k_\mathfrak{p}^*$ 替换 $\mathfrak{p}$ 处的单位群。这样，我们便可以在 Artin 的问题基础上补充两个自然的问题，得到以下三个问题：对于一个数域 K，确定满足以下条件的素数集合 $\mathfrak{p}$ 在 K 中的无穷性（或自然密度）：

I.（Artin）给定元素 $x \in K^*$ 是模 $\mathfrak{p}$ 的本原根，即 $k_\mathfrak{p}^* = \langle \overline{x} \rangle$；II.（Serre [15]）给定椭圆曲线 E/K 模 $\mathfrak{p}$ 具有循环约化；III.（Lang-Trotter [8]）给定点 $P \in E(K)$ 生成群 $E(k_\mathfrak{p})$，当 $\mathfrak{p}$。

Date: 2023年4月11日。2010 *Mathematics Subject Classification.* 主类号 11G05; 次类号 11F80。*Key words and phrases.* 椭圆曲线、本原点、伽罗瓦表示。

我们将情形 I、II 和 III 分别称为乘法原根情形、循环约化情形和椭圆曲线本原根情形，并将相应的素数集合分别记为 $S_{K,\,x}$, $S_{E/K}$ 和 $S_{E/K,\,P}$。根据定义，我们从这些集合中排除有限多个坏约化素数；对于这些素数，$\mathrm{ord}_{\mathfrak{p}}(x) \neq 0$ （情形 I）或 $\mathrm{ord}_{\mathfrak{p}}(\Delta_E) \neq 0$（情形 II 和 III，其中 Δ_E 是 E 的判别式）。注意，显然有包含关系 $S_{E/K,\,P} \subset S_{E/K}$。

在这三种情形中的每一种情形下，我们都有一个群论命题，可以针对 ℓ 群的阶的素因子 $k_{\mathfrak{p}}^*$ 和 $E(k_{\mathfrak{p}})$逐一检验。命题“在 ℓ处”可以用 $\mathfrak{p}$ 在有限伽罗瓦扩张 $K \subset K_\ell$ 中的分裂行为来表述，我们将在第2节对此进行说明。结合所有 ℓ 的要求，可得到基于切博塔廖夫密度定理的（猜想性）密度结论 [16]。

施加无穷多个分裂条件（对每个素数 ℓ施加一个）会带来分析问题，其中的误差项在广义黎曼猜想假设下已在情形 I [1,5,9] 和情形 II [2,3,15], 中得到处理，而在情形 III 中仍未解决。每种情形下，都有一个猜想的密度 $\delta_{K,\,x}$, $\delta_{E/K}$，或$\delta_{E/K,\,P}$，它是素数集合 $\mathfrak{p}$上密度的上界。若猜想的密度为正，无条件证明该集合是无穷集仍是一个开放问题。不过，若其为零，我们可以无条件证明相应的素数集合是有限集。

本文聚焦于椭圆曲线本原根情形下$\delta_{E/K、\,P}$ 的消失问题，这比情形 I 和 II 中的消失问题微妙得多。若一个全局点 $P \in E(K)$ 是局部非本原的，则它仅对有限多个素数而言是局部点群的生成元 $E(k_{\mathfrak{p}})$ $\mathfrak{p}$ 。 K我们的分析将给出定理1.1的“椭圆曲线反例”（E/K， P），即椭圆曲线 E/K的循环约化密度 $\delta_{E/K}$ 为正，但存在一个全局本原点$P \in E(K)$ 是局部非本原的。

与乘法原根情形以及循环约化情形 I 和 II 一样，点 $P \in E(K)$ 的局部本原性阻碍会显现在相关的伽罗瓦表示中。在椭圆曲线本原根情形下，数域 K 的绝对伽罗瓦群 G_K =$\mathrm{Gal}(\overline{K}/K)$ 作用于 $E(\overline{K})$ 的子群，该子群由满足 $kQ \in \langle P \rangle \subset E(K)$ 的点 $Q \in E(\overline{K})$ 构成，其中 $k \in \mathbf{Z}_{\geq 1}$。这给出一个表示$\rho_{E/K,P}$： $G_K \to \mathrm{GL}_3(\mathbf{Z})$。与另外两种情形一样， [2], 只需考虑剩余表示

$$\overline{\rho}_{E,P} : G_K \to \mathrm{GL}_3(\widehat{\mathbf{Z}}) \to \mathrm{GL}_3(\mathbf{Z}/N\mathbf{Z}) \tag{1}$$

模一个适当的无平方因子整数 N，该整数可被所有“临界素数”整除。

与情形 I 和 II 不同，情形 III 在素数层级 $N = \ell$ 上已经允许出现非平凡的局部本原性阻碍。在乘法情形 I 中，对于几乎所有 $\mathfrak{p}$，指数 $[k_{\mathfrak{p}}^* : \langle \overline{x} \rangle]$ 只有在“平凡原因”下才会被 ℓ 整除： K 含有一个 ℓ 次单位根，且 x 是 K^* 中的一个 ℓ 次幂。在循环约化情形 II 中，对于几乎所有 $\mathfrak{p}$，群 $E(k_{\mathfrak{p}})$ 只有在“平凡原因”下才会有非循环的 ℓ 部分：E/K 的全部 ℓ-挠点都是 K-有理的。然而，在椭圆曲线本原根情形 III 中，还有第三种原因会导致点 $P \in E(K)$ 局部ℓ非本原，即对除有限多个 $\mathfrak{p}$ 以外的所有 $\mathfrak{p}$， ℓ 都整除指数 $[E(k_{\mathfrak{p}})$。这种情形不那么显而易见，并于 2015 年由 Meleleo 在 $\ell = 2$ 的情形中通过数值计算发现；他将研究范围限定于基本情形 $K = \mathbf{Q}$。

定理 1.2. 设 $P \in E(K)$ 是定义在数域 K 上的椭圆曲线 E 的一个非挠点，且 ℓ 是素数。那么， P 局部 ℓ非本原，当且仅当以下条件中至少有一个成立

A. $E(K)$ 含有一个阶为 ℓ 的挠点，且 $P \in \ell \cdot E(K)$；B. E 在 K 上具有完全有理的 ℓ-挠；C. 存在一个定义在 K 上的同源 $\phi\colon E' \to E$，其核由 $E'(K)$ 中阶为 ℓ 的挠点生成，且 $P \in \phi[E'(K)]$。

定理1.2中的条件A是情形I 中平凡条件的类比：如果$E(K)$具有非平凡的 ℓ-挠，那么几乎所有 $E(k_{\mathfrak{p}})$都是阶可被 ℓ整除的群，对于这些 $\mathfrak{p}$，点 $P \in \ell \cdot E(K)$ 的约化将位于子群$\ell E(k_{\mathfrak{p}}) \subset E(k_{\mathfrak{p}})$ 中，该子群的指数可被 ℓ整除。条件B 与 P无关，并且在情形II 中广为人知：全局挠子群$E(K)^{\mathrm{tor}}$ 的 ℓ-部分的非循环性意味着 $E(k_{\mathfrak{p}})$的 ℓ-部分在几乎所有 $\mathfrak{p}$处都是非循环的。在这些 $\mathfrak{p}$处，没有单个点 P 能够生成它。

条件 C 在乘法原根情形中没有对应物，而且这是一个真正不同的条件，因为它包含同时有 $P \notin \ell \cdot E(K)\widehat{}$和 $E[\ell](K) = 0$的情形。如果它成立，则对偶同源 $\phi : E \to E'$ 将 P 映射到 $\ell E'(K)$，$\widehat{}$并且对(E, P) 与满足条件 A的曲线-点对$(E', \phi(P))$是 ℓ- 同源的。若条件 C 成立但条件 A 或 B 不成立，我们称局部 ℓ- 非本原的非挠点 $P \in E(K)$ 是非平凡的。

根据定理 1.2，非平凡的局部 2-非本原点 $P \in E（K）$只能存在于 E/K 具有唯一一个 K-有理的 2 阶点，即一个阶为 # 的 2-扭点子群$E（K）[2] \neq 1$，4. 这类点的例子实际上出人意料地丰富。

定理 1.3. 设 E/K 是任意一条满足 $\#E(K)[2] = 2$ 的椭圆曲线。那么， E 在 K 上存在无穷多个二次扭曲，它们都具有非平凡的局部 2- 非本原点。

我们在第 5 节给出该定理的证明。证明利用了这样一个事实：在 E 的扭曲上构造非挠点很容易，并充分利用了 K-有理 2-同源的特别明确的描述。

对于素数 $\ell > 2$，要获得具有无限阶点且以非平凡方式局部 ℓ-非本原的椭圆曲线族则更为困难。第 6 节中，我们针对情形 $\ell = 3$ 给出一种方法。该方法可以推广到更高的 ℓ 值（第 7 节），但例子很快就会变得繁复难解。

确实存在局部非本原、但对任何单个素数 ℓ 都不是局部 ℓ -非本原的非挠点，但这类点并不容易找到。它们涉及由 $\rho_{E/K}$ 的约化所产生的限制，P 以及由不同层级的复合所导致的限制，这些限制源于字段纠缠 于字段 K_ℓ 之间。在较简单的循环约化情形 II 中， [2], 对此已有讨论；在最后的第 8 节中，我们将为 Lang-Trotter 情形 III 给出第一类例子。此类更高层级的阻碍将在即将发表的论文中作更详细的探讨。

致谢。所有作者在撰写本文期间均获得了波恩马克斯·普朗克数学研究所的支持。他们感谢该研究所提供的资金支持以及极富启发性的氛围。

2. Characterization by splitting conditions

对于引言中讨论的三种情形，我们可以根据其元素在适当扩张中的分裂行为，刻画相应的素数集合 $S_{K,\,x}$, $S_{E/K}$ 和 $S_{E/K,\,P}$；其中，K 遍历所有素数。

I. 乘法原根情形。设 K 为一个数域，且 $x \in K^*$为非挠元素。对于 $m \in \mathbf{Z}_{\geq 1}$，将 $K_m = \mathbf{Q}(\zeta_m, \sqrt[m]{x})$ 定义为“ x的 m-除法域”，即多项式 $X^m - x \in K[X]$在 K 上的分裂域。若 $\mathfrak{p}$ 是 K 中一个特征为 p 的素数，且 x 是一个 $\mathfrak{p}$-进单位，则指数 $[k_{\mathfrak{p}}^* : \langle \overline{x} \rangle]$ 可被素数 $\ell \neq p$ 整除，当且仅当 $\mathfrak{p}$ 在 $K \subset K_\ell$中完全分裂。

注意，尽管 $\mathfrak{p}$ 可能在 K_p中完全分裂，$[k_{\mathfrak{p}}^* : \langle \overline{x} \rangle]$ 却从不被 $p = \mathrm{char}(\mathfrak{p})$ 整除。例如：$x = 17$ 是数域 $K = \mathbf{Q}(\sqrt{-21})$ 中范数为 3 的素数 $\mathfrak{p}_3$ 模下的本原根，但 $\mathfrak{p}_3$ 在六次扩张中完全分裂

$$K \subset K_3 = K(\zeta_3, \sqrt[3]{17}) = K(\sqrt{7}, \sqrt[3]{17}).$$

然而，这种情况只可能发生在素数 $\mathfrak{p} | 2\Delta_K$ 上，其中 Δ_K 是 K 的判别式，因为对于与 $2\Delta_K$ 互素的所有 $\mathfrak{p}|p$，$K \subset K_p$ 都在 p 处发生分歧。换言之，对于几乎所有 $\mathfrak{p}$，下述引理中的“在 ℓ 处的条件”在 $\ell = \mathrm{char}\,\mathfrak{p}$ 处自动满足。

引理 2.1. 对于 K 中支集不包含于 x 的素数 $\mathfrak{p}$，当且仅当对于任意素数 $\ell \neq \mathrm{char}\,\mathfrak{p}$，$\mathfrak{p}$ 不在 $K \subset K_\ell$ 中完全分裂时，才有 $k_{\mathfrak{p}}^* = \langle \overline{x} \rangle$。□

根据引理 2.1，集合 $S_{K,\,x}$ 中的素数 K 使得 x 是本原根的素数，除去有限多个素数后，恰好等于对任意素数 $K \subset K_\ell$，在 ℓ中不完全分裂的素数集合。对于 $m \in \mathbf{Z}_{\geq 1}$，在 K 中 $\mathfrak{p}$ 完全分裂的 $K \subset K_m$ 素数集合的自然密度为 $1/[K_m : K]$。在广义黎曼猜想下，由 [9] 可知，集合$S_{K,\,x}$ 具有自然密度，该密度由容斥和给出

$$\delta_{K,x} = \sum_{m=1}^{\infty} \frac{\mu(m)}{[K_m : K]} \tag{2}$$

它收敛得较慢，但可以改写成“因子分解形式”：

$$\delta_{K,x} = \sum_{m|N} \frac{\mu(m)}{[K_m : K]} \cdot \prod_{\ell \nmid N \text{ prime}} \left(1 - \frac{1}{\ell(\ell-1)}\right). \tag{3}$$

这里，N 可以取为一个被某个临界素数有限集中的素数整除的整数。这个有限集可以取为满足以下条件的素数集：这些素数属于 x 的支集，或整除 $2\Delta_K$；此外，还包括那些使得 x 属于 $K^{*\ell}$的素数 ℓ。N 的关键特征在于，族 $\{K_\ell\}_{\ell \nmid N}$ “ x在 N之外的ℓ-除法域”是 K 上的一个线性互不相交族，其中每个 K_ℓ 都具有完整的伽罗瓦群 $\mathrm{Gal}(K_\ell/K) \cong \mathrm{Aff}_1(\mathbf{F}_\ell) = \mathbf{F}_\ell \rtimes \mathbf{F}_\ell^*$，其阶为 $\ell(\ell-1)$；并且该族中各域的合成域 L 满足 $L \cap K_N = K$。

II. 循环约化情形。对于椭圆曲线 E/K，我们考虑 E 的循环约化素数集合 $S_{E/K}$，即满足 E 具有良约化且约化椭圆曲线点群 $E(k_{\mathfrak{p}})$ 为循环群的 K 中的素数 $\mathfrak{p}$。E 在模 $\mathfrak{p}$ 下具有良约化的条件，仅排除了整除 E 的判别式 Δ_E 的有限多个素数。

对于 $m \in \mathbf{Z}_{\geq 1}$，我们将此情形下的 $K_m = K(E[m](\mathbf{Q}))$ 定义为 m-除法域，它是 E 在 K 上的除法域。以下初等引理 [2, 推论 2。2] 是引理 2.1 的类似结果。它表明，有限阿贝尔群是循环群，当且仅当它的 ℓ-主部分对所有素数 ℓ 都是循环群。

引理 2.2. 椭圆曲线 E/K 的一个良约化素数 $\mathfrak{p}$ 是循环约化素数，当且仅当对于任意特征为 $\mathfrak{p}$的素数 $\ell \neq$ ， $\mathfrak{p}$ 在 $K \subset K_\ell$ 中不完全分裂。□

与乘法情形 I 一样，群 $E(k_\mathfrak{p})$ 的 p-主部分的循环性对于特征为 $\mathfrak{p}$的 $p =$ 是自动成立的。这里， $\mathfrak{p}$ 在非平凡扩张$K \subset K_p$ 中完全分裂的情况也确实会发生：只需对任意具有非平凡 $K \subset K_p = K[X]/(f)$ 的椭圆曲线 E/K作基变换，所用扩张为 $K \subset L = K[X]/(g)$，其中 f和 g 是次数相同且在 $\mathfrak{p}$-进意义下足够接近的多项式，但在一个于 $K \subset K_p$中非分歧的素数 $\mathfrak{q}$ 处， g 为艾森斯坦多项式。对于 E/L，非平凡扩张$L \subset L_p$ 将在所有整除 $\mathfrak{p}$的素数处完全分裂。同样，这种情况只能发生在素数 $\mathfrak{p}|2\Delta_K$处；否则，根据 K_p 包含 ζ_p这一事实， $K \subset K_p$ 将在所有特征为 p 的素数 $\mathfrak{p}$ 处均分歧。因此，对于几乎所有 $\mathfrak{p}$，引理 2.2 中的“ ℓ处的条件”在特征为 $\mathfrak{p}$的 $\ell =$ 处又自动成立。显然，在讨论集合 $S_{E/K}$的密度时，整除 $2\Delta_K$ 的有限多个素数无关紧要；该集合与前一种情形一样，除有限多个素数外，与满足以下条件的 K 的素数集合 $\mathfrak{p}$ 重合：对于任意素数 ℓ，这些素数在 $K \subset K_\ell$ 中都不完全分裂。

在广义黎曼猜想成立的条件下，的密度 $S_{E/K}$ 再次由 [2, 第 2] 节中的容斥和给出，我们已经从（2）中得知：

$$\delta_{E/K} = \sum_{m=1}^{\infty} \frac{\mu(m)}{[K_m : K]}. \tag{4}$$

如果 E 在有理数域上没有复乘，或者具有由某个序 $\mathcal{O} \subset K$给出的因式分解 $\delta_{E/K}$ 在排版上与（2）完全相同，前提是N 被适当定义的临界素数有限集中的所有素数 [2, 定理 1.1 和 1.2]。如果 E 具有由某个序 $\mathcal{O} \not\subset K$，则有一个混合公式 [2, 定理 1。4] 其中普通素数和超奇异素数的贡献不同。

关于δ_K的“因式分解公式”x 和 $\delta_{E/K}$ 如（3）所示表明，这些密度的消失总是由某个有限层级 N上的阻碍所导致。对于这样的 N，Gal(K_N/K) 中没有任何元素对所有 $\ell|N$ 限制为 Gal(K_ℓ/K) 中的非平凡元素。因此，在 $S_{K、x}$ 或 $S_{E/K}$中不存在非临界素数：此类素数在 Gal(K_N/K) 中的弗罗贝尼乌斯元素由于群论上的原因不可能存在。

在素数层级 $N = \ell$ 处的一个阻碍，即等式 $K = K_\ell$，在情形 I 和 II 中，归结为我们在定理 1.2 中关于条件 A 和条件 B 的语境下已经提到的一个“平凡”原因。对于 $K =$有理数域，$\delta_{\mathbf{Q},x}$ 和 $\delta_{E/\mathbf{Q}}$的消失仅在我们有 $K = K_\ell$ 且 ℓ 为素数时才会发生；在此情形下，该素数必须是 $\ell = 2$。

在一般数域上，消失可能是由仅仅发生于合数层的阻碍所致。典型例子可以通过将一个不消失的例子基变换（K， x）构造出来，或者将 E/K 基变换到一个合适的扩域 $K \subset L$。例3.1 通过在层$\delta_{K,\ x}$ 处设置阻碍，使 $30 = 2 \cdot 3 \cdot 5$ 在域 $K =$ 有理数域$(\sqrt{5})$ 上消失；通过巧妙选择 x，该阻碍不会出现在较低层。[2，在例 54] 中，我们将椭圆曲线 $E/$有理数域基变换到一个 K 次数为 48 的域，得到一个类似的层 30 阻碍，阻止循环约化。

III. 椭圆曲线本原根情形。除了椭圆曲线 E/K 外，现在还给定一个无限阶点 $P \in E(K)$。我们考虑素数集合 $S_{E/K,\,P}$ 其中的素数 $\mathfrak{p}$ 属于 K，满足 E 具有循环约化，且点 P模 $\mathfrak{p}$ 的约化生成群 $E(k_\mathfrak{p})$。注意显然的包含关系 $S_{E/K,\,P} \subset S_{E/K}$。

对于 $m \in \mathbf{Z}_{\geq 1}$，令 $K_m = K(m^{-1}P)$ 表示 P 的 m-除法域，即由 $E(\overline{K})$ 的子群中的点生成的 K 的扩张，该子群定义为

$$\langle m^{-1}P\rangle = \{Q \in E(\overline{K}) : mQ \in \langle P\rangle\}.$$

注意到，这个扩张 K_m 包含椭圆曲线 E 的 m-除法域，而我们在循环约化情形 II 中遇到过这条曲线。对于 K 中与 m 互素且具有良约化的素数 $\mathfrak{p}$，P 的 m-除法域 $K_m = K(m^{-1}P)$ 在这些素数处仍然非分歧。证明这一事实的方法与证明 E的 m-除法域的非分歧性相同：生成 K_m 在 K 上的 P的 m 次根 $Q \in E(\overline{K})$ 彼此相差 m-挠点，因此它们模一个位于 $\mathfrak{p}$ 上方的素数约化后仍然不同，所以惯性群在这类 Q 的集合上平凡作用。

商群 $V_m = \langle m^{-1}P\rangle/\langle P\rangle$ 是一个在 $\mathbf{Z}/m\mathbf{Z}$ 上秩为 3 的自由模。它带有绝对伽罗瓦群 G_K 对有理数域 K 的自然线性作用，而这个模-m 伽罗瓦表示诱导出一个嵌入

$$G_m = \mathrm{Gal}(K_m/K) \hookrightarrow \mathrm{GL}(V_m) \cong \mathrm{GL}_3(\mathbf{Z}/m\mathbf{Z}). \tag{5}$$

由于 G_K 稳定秩为 2 的子空间 $U_m = E[m](\overline{K}) \subset V_m$，这是一个“可约”表示。记 $V_m = U_m \oplus (\mathbf{Z}/m\mathbf{Z}) \cdot \overline{Q}$，其中 $\overline{Q} = (Q \bmod \langle P\rangle) \in V_m$ 是满足 $mQ = P$ 的点 $Q \in E(\overline{K})$ 的像。于是我们有一个分裂正合列

$$0 \to U_m \longrightarrow V_m \longrightarrow \mathbf{Z}/m\mathbf{Z} \cdot \overline{Q} \to 0$$

由自由 $\mathbf{Z}/m\mathbf{Z}$-模构成；当且仅当满足 $P \in m \cdot E(K)$ 时，该正合列作为 $(\mathbf{Z}/m\mathbf{Z})[G_m]$-模的正合列分裂。选取 U_m 的一个 $\mathbf{Z}/m\mathbf{Z}$-基 $\{T_1, T_2\}$，并用如上所述的某个 $\overline{Q}$ 将其扩充为 V_m 的一个 $\mathbf{Z}/m\mathbf{Z}$-基后，$\sigma \in G_m$ 的矩阵表示变为

$$\sigma = \sigma_{A,b} = \begin{pmatrix} a_{11} & a_{12} & b_1 \\ a_{21} & a_{22} & b_2 \\ 0 & 0 & 1 \end{pmatrix}, \tag{6}$$

其中，σ 在 U_m 上相对于 U_m 的某个 $\mathbf{Z}/m\mathbf{Z}$-基 $\{T_1, T_2\}$ 的线性作用由 $A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \in \mathrm{GL}(U_m)$ 描述，并且

$$b = b_1T_1 + b_2T_2 = \sigma Q - Q$$

是相对于同一基底，对 P 的某个选定的“m 次根” Q 所施加的 σ 的平移作用。换言之，V_m 给出了 G_K 的一个伽罗瓦表示，其像为 $G_m \subset \mathrm{GL}(V_m)$，且包含在二维仿射群中

$$\mathrm{Aff}_2(\mathbf{Z}/m\mathbf{Z}) = (\mathbf{Z}/m\mathbf{Z})^2 \rtimes \mathrm{GL}_2(\mathbf{Z}/m\mathbf{Z}).$$

在 $m = \ell$ 为素数的重要情形下，我们处于有限域 $\mathbf{F}_\ell$ 上的三维伽罗瓦表示这一经典情形。

椭圆曲线本原根情形下，引理 2.1 和2.2 的类比结果稍微复杂一些。我们必须对所有特征为 $\ell \neq$ 、$\mathfrak{p}$ 不等于特征$_\ell \in G_\ell$的素数处的弗罗贝尼乌斯元素 $\mathrm{Frob}_\mathfrak{p}$, $_\ell \in G_\ell$ 施加一个条件：在这种情形下，只需要求它与单位元 $\mathrm{id}_\ell \in G_\ell$“足够接近”。

引理 2.3. 对于无限阶的 $P \in E(K)$，以及特征不同于 ℓ的 E的一个良约化素数 $\mathfrak{p}$，我们有

$$\ell | [E(k_\mathfrak{p}) : \langle \overline{P} \rangle] \quad \Longleftrightarrow \quad \operatorname{rank}(\mathrm{Frob}_{\mathfrak{p},\ell} - \mathrm{id}_\ell) \leq 1.$$

证明。由于所有 V_ℓ 在 $\mathbf{F}_\ell$ 上都是 3 维的，条件 $\operatorname{rank}(\mathrm{Frob}_{\mathfrak{p},\ell} - \mathrm{id}_\ell) \leq 1$ 意味着 $\mathrm{Frob}_{\mathfrak{p},\ell}$ 在 V_ℓ 的一个 $\mathbf{F}_\ell$-子空间上恒等，该子空间的维数至少为 2。若它等于 U_ℓ，则 $E(k_\mathfrak{p})$ 具有完整的 ℓ-挠，阶为 ℓ^2，且每个循环子群 $\langle \overline{P} \rangle$ 的指数都可被 ℓ 整除。若非如此，它与 U_ℓ 相交于一个 1 维子空间，因此我们在 $E(k_\mathfrak{p})$ 中有一个阶为 ℓ 的点，以及一个满足$\ell \overline{Q} = \overline{P}$的点 $\overline{Q} \in E(k_\mathfrak{p})$。这也意味着 $[E(k_\mathfrak{p}) : \langle \overline{P} \rangle]$ 可被 ℓ 整除。

反过来，若 ℓ 可整除 $[E(k_\mathfrak{p}) : \langle \overline{P} \rangle]$，则要么 $E(k_\mathfrak{p})$ 具有完整的 ℓ-挠，要么 $E(k_\mathfrak{p})$ 具有一个非平凡的循环 ℓ-部分，且 $\overline{P}$ 包含于 $\ell \cdot E(k_\mathfrak{p})$。在这两种情况下，$\mathrm{Frob}_{\mathfrak{p},\ell}$ 在 V_ℓ 的一个子空间上恒等，该子空间的维数至少为 2。□

推论 2.4。设 $P \in E(K)$ 为无限阶，且 $\mathfrak{p}$ 是 E 的素数范数良约化素数，$\mathrm{char}\ \mathfrak{p} > 5$，满足 $\overline{P} \neq \overline{O} \in E(k_\mathfrak{p})$。则有

$$E(k_\mathfrak{p}) = \langle \overline{P} \rangle \quad \Longleftrightarrow \quad \operatorname{rank}(\mathrm{Frob}_{\mathfrak{p},\ell} - \mathrm{id}_\ell) \geq 2 \ \textit{for all primes}\ \ell.$$

证明。根据引理2.3，右侧的条件表明，$p = \mathrm{char}\,\mathfrak{p}$ 是指数 $[E(k_\mathfrak{p}): \langle \overline{P} \rangle]$的唯一可能的素数因子。对于次数为一的素数 $\mathfrak{p}$，即具有素数范数 p的素数，$E(k_\mathfrak{p}) = E(\mathbf{F}_p)$ 的一个子群的指数只有在它是平凡子群时才可能被 p 整除，因为对于 $p > 5$，我们有$\#E(\mathbf{F}_p) < p + 1 + 2\sqrt{p} < 2p$。因此，除非 $\mathfrak{p}$ 是一个满足 $\overline{P} = \overline{O} \in E(k_\mathfrak{p})$ 的素数，否则我们有 $E(k_\mathfrak{p}) = \langle \overline{P} \rangle$。由于我们有 $P \neq O \in E(K)$，这只会对有限多个 $\mathfrak{p}$ 发生。□

在密度问题中，我们可以忽略任何有限集的素数，更一般地，也可以忽略一个密度为零的素数集。次数大于一的数域中的素数集就是这样一个零密度集。因此，集合 $S_{E/K,\ P}$的密度只取决于它所包含的任意有限集“临界素数”之外的次数为一的素数。因此，推论2.4 可以发挥与引理2.1和2.2相同的作用。

为了表示 $S_{E/K,\ P}$ 的“启发式密度”$\delta_{E/K,\ P}$，我们将 $S_\ell \subset G_\ell = \mathrm{Gal}(K_\ell/K)$ 定义为在素数 ℓ 处的“坏”元素子集

$$S_\ell = \{\sigma \in G_\ell : \operatorname{rank}_{\mathbf{F}_\ell}(\sigma - \mathrm{id}_\ell) \leq 1\}.$$

对于任意 $m \in \mathbf{Z}_{\geq 1}$ 和 $\ell | m$ 素数，我们令 $\pi_{m,\ell} : G_m \to G_\ell$ 为自然限制映射，并定义 $S_m \subset G_m$ 为

$$S_m = \bigcup_{\ell | m} \pi_{m,\ell}^{-1}[S_\ell].$$

以 $s_m = \#S_m$ 表示 S_m的基数，椭圆原根密度现在由容斥和给出

$$\delta_{E,P} = \sum_{m=1}^{\infty} \frac{\mu(m) s_m}{[K_m : K]}. \tag{7}$$

它是乘法原根密度的椭圆曲线类比（2）。它是 $S_{E/K,P}$ 的上密度；在 $\delta_{E/K,P} > 0$ 的情形下，尚未证明它就是实际密度，即使假设广义黎曼猜想也未能证明。

我们可以用$\delta_{E/K,P}$ 的方法来计算 [2]。这与本文的重点并不直接相关，因为我们关注的是 $\delta_{E/K,P}$ 以“非平凡”方式消失的情形，因此这里只作简要概述。为了得到一个因式分解

$$\delta_{E/K,P} = \sum_{m|N} \frac{\mu(m)s_m}{[K_m : K]} \cdot \prod_{\ell\nmid N \text{ prime}} (1 - \frac{s_\ell}{[K_\ell : K]}). \tag{8}$$

如（3）所示，只需对伽罗瓦表示$\rho_{E,\ P}$（由 G_K 对子群的作用产生）证明开像定理

$$R_P = \{Q \in E(\overline{K}) : mQ \in \langle P\rangle \text{ for some } m \in \mathbf{Z}_{\geq 1}\} \cong (\mathbf{Q}/\mathbf{Z})^2 \times \mathbf{Q}$$

$E(\overline{K})$ 中由 $E(\overline{K})$ 内 P 的所有根生成的子群。G_K 对商群 $V = R_P/\langle P\rangle$ 的伽罗瓦作用给出了一个伽罗瓦表示；该商群作为 Q/Z 上的模是秩为 3 的自由模，

$$\rho_{E,P} : G_K \longrightarrow \mathrm{Aut}(V) \cong \mathrm{GL}_3(\widehat{\mathbf{Z}}),$$

它的模 m 表示就是 (5)。它经由 Gal$(K(R_P)/K)$ 分解，其中 $K(R_P)$ 是 $\overline{K}$ 内 P 的所有“m-除法域”的合成域。群 $U = E(\overline{K})^{\mathrm{tor}} \cong$ (Q/Z)^2 是 V 的直和项；若像处理 $V_m = U_m \oplus$ Z$/m$Z$\cdot \overline{Q}$ 时那样，为 $V = U \oplus$ Q/Z 选取一个 Q/Z-基，则 $\rho_{E,P}$ 的像属于 Aff$_2(\widehat{\ }$Z$) = \widehat{\ }$Z$^2 \rtimes$GL$_2(\widehat{\ }$Z$)$。对于在 $\overline{K}$ 上无复乘的 E，由 Serre 的$\widehat{\ }$开像定理可知，该像在 Aff$_2$(Z) 中具有有限指数，由此可得，对于任意可被临界素数 $_P \in$Z$_{>0}$ 的某个有限乘积整除的 N，结论 (8) 成立。如 [2], 所示，可推得所有非复乘密度 $\delta_{E,P}$ 都是某个普适常数 $\widehat{\ }$ 的有理数倍。若 E 在 $\overline{K}$ 上具有由阶 $\mathcal{O} \subset K$ 给出的复乘，则以 Aff$_1(\mathcal{O})$ 取代 Aff$_2$(Z)；若复乘由阶 $\mathcal{O} \not\subset K$ 给出，则如 [2] 所示，将 E/K 的普通素数和超奇异素数的贡献分开处理。

3. Multiplicative primitivity

在讨论 Lang-Trotter 情形 III 之前，我们先解决乘法本原根情形：在广义黎曼猜想成立的条件下，全局原始元素 $x \in K^*$ 对于一组具有正密度的素数$\delta_{K,\ x}$是局部原始的。

定理 *1.1* 的证明。设 $x \in K^*$ 是全局本原的。由于我们假设广义黎曼猜想成立，$x \in K^*$ 的原根密度存在，且等于 $\delta_{K,\ x}$ 其定义见（2），这是由 [9]的结果得出的。我们需要证明 $\delta_{K,\ x}$ 不为零。根据因式分解公式（3），只需证明：对于任意无平方因子整数$N > 1$，分数 $\sum_{m|N} \mu\ (m)\ [K_m :\ K]^{-1}$ 在 Gal(K_N/K) 中，对所有素数 K_ℓ 在 $\ell|N$ 上的限制均非平凡的元素所占比例不为零。

由于 x 不是 K^*中的 ℓ次幂，多项式 $X^\ell - x$ 在 $K[X]$中不可约。因此它给出一个扩张 $K \subset K_\ell =$ Split$_K(X^\ell - x) = K(\zeta_\ell, \sqrt[\ell]{x})$，其次数为 $\ell\cdot c_\ell$，其中 c_ℓ 是 $\ell - 1$的一个因子。若 ℓ 是无平方因子整数 N的最大素因子，则可得 $K_{N/\ell} \subset K_N$ 是伽罗瓦扩张，且其次数可被 ℓ整除。

现在，只需对整除无平方因子整数 $N > 1$ 的素数个数进行归纳，即可轻松证明 Gal(K_N/K) 含有一个具有所需类型的元素。如果 N 是素数，那么 Gal(K_N/K) 含有一个非平凡的 N 阶元素。否则，令 ℓ 为整除 N 的最大素数，并注意到，归纳假设表明 Gal$(K_{N/\ell}/K)$ 中存在一个具有所需类型的自同构，而它总是

可以扩张到 $K_{N/\ell}$ 与 K_ℓ 的合成域 K_N 上，且在 K_ℓ 上非平凡。□

定理 1.1 中的全局本原性假设不能弱化为假设 $K \neq K_\ell$ 对所有素数 ℓ均成立。这个更强的陈述对 $K =$ 有理数域是正确的，但对一般数域 K而言存在反例，因为对于不同的 $K \subset K(\zeta_\ell$，分圆扩张 ℓ 可能都非平凡，却在 K上彼此“纠缠”。下面的反例取 K 为二次的。

例3.1. 二次域 $K =$ 有理数域$(\sqrt{5})$具有基本单位 $\varepsilon = \frac{1+\sqrt{5}}{2}$。元素 $\pi = \varepsilon^2 - 4 = \frac{-5+\sqrt{5}}{2} \in K$ 的范数为5，且模 4 为平方。因此，域 $K(\sqrt{\pi})$ 是有理数域上的 4次循环的扩张，除 5 外均非分歧，故等于 $K(\zeta_5)$。取 $y = -3\pi \in K$ 并选择 $x = y^{15}$。于是我们有

$$K_3 = K(\zeta_3) = K(\sqrt{-3}) \qquad \text{and} \qquad K_5 = K(\zeta_5) = K(\sqrt{\pi}),$$

因此， $K_2 = K(\sqrt{x})$、 $= K(\sqrt{y})$、 $= K(\sqrt{-3\pi})$以及 K_3 和 K_5 是包含在双二次扩张 $K \subset K_6 = K_{10} = K_{15} =$$K_{30}$中的 K 的三个不同二次扩张。我们有 $\mu_K = \{\pm 1\}$，而尽管 x 不是 K^*中的平方，但恰好有一个 K 的素数模使得 x 是本原根：(2)。对于素数 $\mathfrak{p} =$(3)和 $\mathfrak{p} = (\sqrt{5})$，元素 x 不属于 $k_\mathfrak{p}^*$；对于特征为 $p > 5$的所有素数，指数 $[\mathbb{F}_p^* : \langle \overline{x} \rangle]$ 至少能被2、3或5中的一个整除。事实上，在群为 $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ 的扩张中，不存在一个素数能在三个二次子域中都保持惰性。

一个简单的观察是，没有任何素数 $\mathfrak{p}$ 属于数域 K 能在扩张 $K \subset L$ 的三个二次子扩张中都保持惰性，其群为 $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ 这一事实构成了许多“纠缠障碍”的基础，包括我们在最后的第8节中讨论的那个。

4. Proof of Theorem 1.2

在Lang-Trotter 情形下，引理 2.3 表明，当 $\mathrm{Frob}_{\mathfrak{p},\ell} \in G_\ell$ 逐点固定 3维 $\mathbb{F}_\ell$-向量空间 V_ℓ的一个2 维子空间时，点 $P \in E(K)$ 将生成局部点群 $E(k_\mathfrak{p})$ 的一个指数可被 ℓ 整除的子群。因此，在 $G_\ell =$Gal(K_ℓ/K) 非平凡、但只包含逐点固定 V_ℓ 的一个 2 维子空间的元素的情形下，密度 $\delta_{E/K,P}$ 可能会“因为K_ℓ”而消失。

我们对定理 1.2 的证明基于一个一般性引理。按照 Hendrik Lenstra 向我们提出的建议，我们以相当一般的形式表述并证明了该引理。它描述了任意域上有限维向量空间上的线性群作用，这些作用具有“许多不动点”，其含义参照我们手头的三维例子 V_ℓ。

设 V 为任意一个由群 G 线性作用的向量空间，并记为

$$V^G = \{v \in V : \sigma v = v \text{ for all } \sigma \in G\} \qquad \text{and} \qquad V_G = V/(\textstyle\sum_{\sigma \in G}(\sigma - 1)V)$$

G 作用平凡的最大子空间与商空间。对每个$\sigma \in G$，我们都有一个向量空间的正合列。

$$0 \longrightarrow V^{\langle\sigma\rangle} \longrightarrow V \xrightarrow{\sigma - 1} V \longrightarrow V/(\sigma - 1)V \to 0$$

表明对于有限维的 V n，我们有

$$\dim V^{\langle\sigma\rangle} \geq n - 1 \quad \Longleftrightarrow \quad \dim(\sigma - 1)V \leq 1. \tag{9}$$

引理 4.1. 设 G 群在线性地作用于维数为$n \in \mathbf{Z}_{\geq 0}$的向量空间 V 上。则以下各项等价：

(1) $\dim V^{\langle\sigma\rangle} \geq n-1$ *for all* $\sigma \in G$;
(2) $\dim V^G \geq n-1$ *or* $\dim V_G \geq n-1$.

证明。 蕴含关系 (2) $\Rightarrow$ (1) 是显然的，因为不等式 $\dim V_G \geq n-1$表明，对所有 $\sigma \in G$，都有 $\dim(\sigma-1)V \leq 1$ 并且根据 (9)，$\dim V^{\langle\sigma\rangle} \geq n-1$。

对于 (1) $\Rightarrow$ (2)，我们可以假设存在 $\sigma \in G$ 在 V 上非平凡作用，并定义子群 A_σ、$B_\sigma \subset G$ 如下：

$$A_\sigma = \{\tau \in G\colon V^{\langle\tau\rangle} \supset V^{\langle\sigma\rangle}\} \qquad \text{and} \qquad B_\sigma = \{\tau \in G\colon (\tau-1)V \subset (\sigma-1)V\}.$$

等式 $A_\sigma = G$表明 $V^G = V^{\langle\sigma\rangle}$的维数为 $n-1$，而等式$B_\sigma = G$ 表明 $V_G = V/(\sigma-1)V$的维数为 $n-1$。为了证明这些等式之一成立，从而得到 (2)，我们通过矛盾来论证。假设A_σ 和 B_σ 是 G的真子群，并选取 $\tau \in G$ 不属于 $A_\sigma \cup B_\sigma$。于是存在 $s \in V^{\langle\sigma\rangle} \setminus V^{\langle\tau\rangle}$ 和 $t \in V^{\langle\tau\rangle} \setminus V^{\langle\sigma\rangle}$，且 $(\sigma-1)V$与 $(\tau-1)V$是 V中不同的一维子空间，分别由 $(\sigma-1)t$ 和 $(\tau-1)s$张成。

子空间 $(\tau\sigma-1)V$是一维的，由$(\tau\sigma-1)s = (\tau-1)s$张成，因此它等于 $(\tau-1)V$。它包含 $(\tau\sigma-1)t = \tau(\sigma-1)t$，但由于 τ对 $(\sigma-1)t \notin (\tau-1)V$的作用是沿着$(\tau-1)V$中的一个向量进行平移，我们有 $\tau(\sigma-1)t \notin (\tau-1)V$。矛盾。 □

对于喜欢用矩阵来理解引理 4.1 的人，条件(1) 意味着 G 中的每个元素相对于某个适当的基都有一个矩阵表示，根据（9），可写成以下等价形式之一

$$\text{(10)} \qquad \begin{pmatrix} \boxed{I_{n-1}} & \begin{matrix}*\\ \vdots \\ *\end{matrix} \\ \begin{matrix}0 & \cdots & 0\end{matrix} & * \end{pmatrix} \qquad \text{or} \qquad \begin{pmatrix} * & * & \cdots & * \\ 0 & & & \\ \vdots & & \boxed{I_{n-1}} & \\ 0 & & & \end{pmatrix}.$$

第一种形式展示了 $n-1$ 直线性无关向量，位于 $V^{\langle\sigma\rangle}$中；第二种形式从一个张成 $(\sigma-1)V$ 的向量开始。该引理随后指出，在此条件下，可以为 V 选取一个单一的基，使得 G 的所有元素要么都具有第一种形式的矩阵表示，要么都具有第二种形式的矩阵表示。

例 4.2. 对于椭圆曲线 E/K，我们可以将引理 4.1 应用于伽罗瓦群 G 在 K 上的 E 的 ℓ-除法域对 E的 ℓ-挠点所构成的 2 维 $\mathbf{F}_\ell$-向量空间 $V = E[\ell](\overline{K})$ 的作用。在此情况下，良约化素数 $\mathfrak{p} \nmid \ell$ 处的点群$E(k_\mathfrak{p})$的阶可被 ℓ 整除，当且仅当 $\mathrm{Frob}_\mathfrak{p} \in G$ 逐点固定 V的一个 1 维子空间。我们发现，几乎所有局部点群 $E(k_\mathfrak{p})$的阶可被 ℓ 整除，当且仅当 G_K 在 E 的 ℓ-挠点群上的伽罗瓦表示 $\rho_{E/K,\ell}$ 可以写成矩阵形式：

$$\rho_{E/K,\ell} \sim \begin{pmatrix} 1 & * \\ 0 & * \end{pmatrix} \qquad \text{or} \qquad \rho_{E/K,\ell} \sim \begin{pmatrix} * & * \\ 0 & 1 \end{pmatrix}.$$

换言之：要么 $E(K)$ 含有一个 ℓ 挠点，要么它在 K 上与一条椭圆曲线 ℓ 同源，而该曲线上有一个 K 有理的 ℓ 挠点。此外，对于第一类的 E/K，若有一个阶为 ℓ 的点 $T \in E(K)$，则商曲线 $E' = E/\langle T\rangle$ 是

第二类，其对偶同源 $E' \to E$ 正是所讨论的 ℓ-同源。这是一个众所周知的事实，也是 [14, 第 I-2] 页最早出现的一道习题。

定理1.2 的证明。设 E/K 为一条椭圆曲线，且 $P \in E(K)$是一个局部 ℓ-非本原的非挠点。我们按照第 2 节定义 $K_\ell = K(\ell^{-1}P)$，并将 $G_\ell = \mathrm{Gal}(K_\ell/K) \subset \mathrm{GL}(V_\ell)$ 视为 $V_\ell = \langle \ell^{-1}P\rangle/\langle P\rangle$ 上的 3 维 $\mathbf{F}_\ell$- 线性自同构群。由于 G_ℓ 中的每个元素都作为无穷多个良约化素数的弗罗贝尼乌斯出现，由引理2.3 可知， G_ℓ 的所有元素都将 V_ℓ 的某个2维子空间逐点保持不变。现在我们可以对 $n = 3$ 应用引理 4.1，结合 $G = G_\ell$ 和 $V = V_\ell$，从而得出以下至少一种情况： G_ℓ 在 V_ℓ的某个2维子空间上平凡作用，或者 G_ℓ 在 V_ℓ 的某个 2 维商空间上平凡作用。

在第一种情形下，若 $U_\ell = E[\ell](\overline{K})$ 是一个 G_ℓ 作用平凡的子空间，则 $E(K)$ 的 ℓ-挠点群是完备的，且满足条件 B。若 G_ℓ 在另一个二维子空间 $S_\ell \subset V_\ell$ 上作用平凡，则 S_ℓ 由 $U_\ell \cap S_\ell$ 中的一个非零向量和 V_ℓ 这个 $\mathbf{F}_\ell$-向量空间中一个无限阶点 $Q \in \langle \ell^{-1}P\rangle$ 的非零像张成。换言之： $E(K)$ 含有一个阶为 ℓ 的挠点，以及一个点 Q，满足对于某个不能被 ℓ 整除的 $\mathbf{Z}$ 中元素 $m \in$，有 $\ell Q = mP$。将 $am + b\ell = 1$ 写作 $\mathbf{Z}$ 中的元素后，点 $Q' = aQ + bP \in E(K)$ 满足 $\ell Q' = a\ell Q + b\ell P = amP + b\ell P = P$，因此条件 A 得以满足。

在第二种情形下， G_ℓ 在二维商空间 V_ℓ/T_ℓ 上作用平凡，因此它沿着一维子空间 T_ℓ 对 V_ℓ 作平移。我们假设 G_ℓ 在子空间 U_ℓ 上的作用并非平凡，否则就会回到第一种情形，并满足条件 B。由于 $U_\ell = E[\ell](\overline{K}) \subset V_\ell$ 是 G_ℓ-稳定的，我们有 $\mathbf{F}_\ell[G_\ell]$-模的严格包含关系 $0 \subsetneq T_\ell \subsetneq U_\ell$，因此 T_ℓ 是 $E(\overline{K})$ 的一个阶为 ℓ 的 K-有理子群。相应的同源 $E \to E' = E/T_\ell$ 定义在 K 上，并将具有平凡 G_ℓ 作用的 $\mathbf{F}_\ell[G_\ell]$-模 U_ℓ/T_ℓ 与 $E'(K)$ 中阶为 ℓ 的子群相对应；该子群是同源 $\phi\colon E' \to E$ 到 $\phi\colon E \to E' = E/T_\ell$ 的核。若 $Q \in E(K)$ 满足 $\ell Q = P$，则 $P' = \phi(Q)$ 属于 $E'(K)$，因为它是伽罗瓦轨道 $G_\ell \cdot Q \subset Q + T_\ell$ 中任意一点的像。此外，我们有 $\phi(P') = \phi\phi(Q) = \ell Q = P$，因此满足定理 1.2 的条件 C。

反过来，条件 A、B 和 C 中的每一个都保证 $P \in E(K)$ 是局部 ℓ-不可约的。对于 A 和 B，这是显然的。若条件 C 成立，则存在一个定义在 K 上的 ℓ-同源 $\phi\colon E' \to E$，以及一个点 $P' \in E'(K)$，满足 $\phi(P') = P$.$\widehat{}$取满足 $\ell Q' = P'$ 的 $Q' \in E'(\overline{K})$，并令 $Q = \phi(Q') \in E(\overline{K})$。记 $\phi\colon E \to E'$ 为对偶同源，我们便处于例 4.2 的情形，并且有

$$\ell Q = \phi(\ell Q') = \phi(P') = P \qquad \text{and} \qquad \widehat{\phi}Q = \widehat{\phi}\phi Q' = \ell Q' = P' \in E'(K).$$

由于 Q 位于纤维 $\widehat{\phi}^{-1}(P')$ 中， G_ℓ 在 Q 模 $\langle P\rangle \in V_\ell$ 上的作用是对 ℓ-挠点进行平移，由此得到一个长度整除 ℓ 的伽罗瓦轨道。若长度为 1，则满足条件 A，且 $P \in E(K)$ 是局部 ℓ-不可约的。若长度为 ℓ，则 G_ℓ 通过沿 K-有理子群 $\backsim T_\ell = \ker\phi \subset U_\ell = E[\ell](\overline{K})$ 平移作用于 V_ℓ，并且相对于滤过 $T_\ell \subset U_\ell \subset V_\ell$， G_ℓ 在 V_ℓ 上的矩阵表示为

$$\rho_{E/K,\ell} \sim \begin{pmatrix} * & * & * \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

根据引理 2.3，我们得到 $\ell|[E(k_\mathfrak{p}):\ \langle\overline{P}\rangle]$ 对每个 $\mathfrak{p}$ 的良约化素数 E，其特征不同于 ℓ，因此 $P \in E(K)$ 是局部ℓ-不可约的。□

5. Locally 2-imprimitive points

椭圆曲线 E/K 上的非平凡局部 ℓ-非本原点是一个非挠点 $P \in E(K)$，它满足定理1.2 的条件 C，但不满足条件 A 或 B。若 P 是这样的点，则 E 存在一个定义在 K 上的有理 ℓ-同源 $E \to E'$，且 G_K 在 $U_\ell = E[\ell](\overline{K})$ 上的伽罗瓦表示 $\overline{\rho}_{E,\ell}$ 非平凡，其像包含于 $\mathrm{GL}(U_\ell)$ 的一个波莱尔子群中。

设 $P \in E(K)$ 是一个非平凡的局部 2-非本原点。由于 $\mathrm{GL}(U_2) \cong \mathrm{GL}_2(\mathbf{F}_2)$ 的波莱尔子群阶为 2，表示$\overline{\rho}_{E,2}$ 是一个非平凡的二次特征；而作为 E 的魏尔斯特拉斯模型，我们可以取

$$E : y^2 = x(x^2 + ax + b) \qquad \text{with } b, d = a^2 - 4b \in K^*. \tag{11}$$

此处 $(0,0)$ 是阶为 2的 K-有理点，而 $\overline{\rho}_{E,2}$ 对应于 E 在 K上的2-除法域，该域等于 $K(\sqrt{d})$。加上 $(0,0)$ 诱导出一个对合

$$(x, y) \mapsto (x_1, y_1) = (b/x, -by/x^2)$$

在 $K(E) = K(x, y)$的函数域上，且不变子域 $K(x+x_1, y+y_1)$是 2-同源曲线 $E' = E/\langle(0,0)\rangle$ 的函数域。选取 $u = x+x_1+a$和 $v = y + y_1$ 作为 $K(E')$ 的生成元，我们得到一个魏尔斯特拉斯模型

$$E' : v^2 = u(u^2 - 2au + d) \qquad \text{with } d, d' = (-2a)^2 - 4d = 16b \in K^* \tag{12}$$

对于 E' 其形式相同（11），以及一个显式的 2-同源 $\varphi:\ E \to E'$ 给出为

$$\varphi : (x, y) \longmapsto (u, v) = (x + x_1 + a, y + y_1) = \left(\frac{y^2}{x^2}, (1 - \frac{b}{x^2})y\right). \tag{13}$$

仿射点 $(u, v) \in E'(K)$ 若不同于 $(0,0)$，则当且仅当 $u \in K^*$ 是平方时，它才属于此同源映射 $E(K)$ 的像。点 $(0,0)$ 属于该像，当且仅当 d 是 K^* 中的平方，这相当于说 $E(K)$ 具有完整的 2-扭点。我们的 E 并非如此。

由于 E' 再次具有（11）的形式，可以看出同源 $\widehat{\varphi}:\ E' \to E$ 是 φ的对偶同源，其形式为

$$\widehat{\varphi} : (u, v) \longmapsto \left(\frac{v^2}{4u^2}, (1 - \frac{b}{u^2})\frac{v}{8}\right). \tag{14}$$

定理 *1.3* 的证明。设 E/K 是一个椭圆曲线，且其 $\#E(\overline{K}) = 2$。在 E 的魏尔斯特拉斯模型中，我们取（0，0）作为 2 阶点，从而得到方程 $E:\ y^2 = x(x^2 + ax + b)$ 如（11）所示，其中 $d = a^2 - 4b \in K^* \setminus K^{*2}$。$E$ 在 K 上的任意二次扭曲都具有以下形式

$$E_D : y^2 = x(x^2 + aDx + bD^2)$$

对于某个 $D \in K^*$，我们仍可通过 K^* 中的平方数对其进行缩放；并且如上所述，将 (11)、(12) 和 (13) 中的 (a, b) 替换为 (aD, bD^2)，即可定义 2-同源 $\varphi:\ E_D \to E'_D = E/\langle(0,0)\rangle$。满足定理 1.2 中条件 C 的任意点 $P \in E_D(K)$ 都属于同源 $\widehat{\varphi}:\ E'_D \to E_D$ 的像 $\widehat{\varphi}(E'_D(K))$，其中该同源是 φ 的对偶同源。这意味着它的 x 坐标是 K^* 中的一个平方数，我们可以将其取为 1，之后。

对 E 在 K上的模型进行重新缩放。因此，对我们而言相关的扭曲，是使点 $P=(1,\pm Y)\in E_D(\overline{K})$ 为 K-有理的那些扭曲。

我们希望(D,Y)是圆锥曲线 $Y^2=1+aD+bD^2$ 上一个不同于$(0,\pm1)$的 K-有理点。此类点可作为该圆锥曲线与经过$(0,1)$ 且斜率为 $\lambda\in K$ 的直线 $Y-1=\lambda D$ 的第二个交点得到。我们发现，扭曲 $E_\lambda=E_{D_\lambda}$ 的 E 通过

$$D_\lambda=\frac{a-2\lambda}{\lambda^2-b}\qquad\text{with }\lambda\in K\setminus\{a/2,\pm\sqrt{b}\} \tag{15}$$

通过构造得到一个 K-有理点

$$P_\lambda=(1,Y_\lambda)=\left(1,\frac{\lambda^2-a\lambda+b}{\lambda^2-b}\right)\in E_\lambda(K). \tag{16}$$

我们可以通过求解 $2Q=\widehat{\varphi}(\varphi Q)=P_\lambda$ in $E_\lambda(\overline{K})$ 来找到 $K_2=K(\frac{1}{2}P_\lambda)$。方程$\widehat{\varphi}(u,v)=P_\lambda$ 在 $E'_\lambda(K)$ 中有 2 个解，因为我们为 P_λ 的第一个坐标选择了平方值 1。根据 (14)，这些是不同于 (0,0) 的 K-有理点 (u,v)，它们具有 $v^2=4u^2$ 并满足方程

$$v^2=u(u^2-2aD_\lambda u+dD_\lambda^2)$$

定义 E'_λ。借助 $d=a^2-4b$，所得方程

$$u^2-2aD_\lambda u-4u+dD_\lambda^2=(u-aD_\lambda-2)^2-4(1+aD_\lambda+bD_\lambda^2)=0$$

对于 u 得到两个解 u_1，$u_2=aD_\lambda+2\pm Y_\lambda\in K$ 其乘积为 $u_1u_2=dD_\lambda^2$。写作 D_λ 以及 P_λ，如式（15）和（16）所示，可得 $aD_\lambda+2-Y_\lambda=d/(\lambda^2-b)$，因此对应点属于 $K\subset K_2$ 的最小扩张 $\varphi[E(K_2)]$ 为

$$K_2=K(\tfrac{1}{2}P_\lambda)=K(\sqrt{u_1},\sqrt{u_2})=K(\sqrt{d},\sqrt{\lambda^2-b}).$$

如果避开以下值 $\lambda\in K$ 使得 λ^2-b 要么是平方数，要么是 d 在 K 中乘以平方数的值——这包括（15）中排除的 3 个值——那么 K_2 是 K 的双二次扩张，正如预期的那样，它具有除法域 $K(\sqrt{d})$ E/K 作为其二次子扩张之一。对于这些 λ，我们根据（5）和（6）得到的 $G_2=\mathrm{Gal}(K_2/K)$ 的矩阵表示变为

$$\mathrm{Gal}(K_2/K)=\left\{\begin{bmatrix}1&x&y\\0&1&0\\0&0&1\end{bmatrix}:x,y\in\mathbf{F}_2\right\},$$

这意味着 $P_\lambda\in E_\lambda(K)$ 是全局 2-本原的，但却是局部 2-非本原的。

仍有一种可能： P_λ 虽然是全局 2-本原的，却是偶数阶 $m>2$ 的挠点。例如，$y^2=x(x^2-7x+3)$ 上的点 $(1,-3)$ 的阶为 4，而 $y^2=x(x^2+3x-3)$ 上的点 $(1,1)$ 的阶为 6。然而，对于固定的 K，根据 Merel 定理，m 只有有限种可能。对于给定的偶数 m，点 P_λ 的阶为 m 当且仅当 m 次除法多项式 $\psi_m(x)=y^{-1}f(x,E_\lambda)$ 在 $x=1$ 处为零。由于在固定 a、$b\in K$ 时，$f(1,E_\lambda)$ 是 λ 的非常数有理函数，因此这只会对 λ 的有限多个值发生。□

我们对局部2-非本原性的理解基本上已经完整，因为椭圆曲线上每个非平凡的2-局部非本原点都源自定理 1.3证明中的构造。事实上，假设 $\#E[2](\overline{K})=2$ 意味着 E 具有形如（11）的模型；又由于满足定理 1.2 的点 P 的 x坐标是平方，因此可以在 K 上缩放该模型，使其满足 $P=(1,y)\in E(K)$。

6. Locally 3-imprimitive points

根据定理 1.2，椭圆曲线 E/K 上每个带有非平凡局部ℓ-非本原点 $P \in E(K)$ 的点对 (E, P) ℓ都是某个 K-有理曲线-点对 (E', P') 在 $E' \to E$ 核由一个 ℓ-挠点 $T \in E'(K)$ 生成的情况下，经 G_K -同源映射得到的像。在这种情况下，相对于适当的基， ℓ在 E' 和 $E = E'/\langle T\rangle$ 的 ℓ-挠子群上的伽罗瓦表示具有如下形式：

$$\rho_{E'/K,\ell} \sim \begin{pmatrix} 1 & * \\ 0 & \omega_\ell \end{pmatrix} \qquad \text{and} \qquad \rho_{E/K,\ell} \sim \begin{pmatrix} \omega_\ell & * \\ 0 & 1 \end{pmatrix}. \tag{17}$$

这里 ω_ℓ 是与扩张 $K \subset K(\zeta_\ell)$相对应的圆分特征。对于$\ell > 2$， K-有理性并不保持 ℓ 的 E -挠点在对E进行扭曲后并不保持，因此不存在定理 1.3 关于 $\ell \neq 2$的直接类似结论。本节聚焦于 $\ell = 3$的情形。

引理 6.1。 设 E/K 是判别式为 Δ_E 且其伽罗瓦表示 $\rho_{E/K,3}$ 在 $U_3 = E[3](\overline{K})$ 上具有 (17)中的两种形式之一的 3椭圆曲线。则 E在 K上的 3-除法域等于多项式 $X^3 - \Delta_E$的分裂域。

证明。设 $H_3 = \mathrm{Gal}(K(E[3])/K) \subset \mathrm{GL}(U_3) \cong \mathrm{GL}_2(\mathbf{F}_3)$ 为 $\rho_{E/K,3}$ 的像，并记 $\psi_3 = \prod_{i=1}^4 (X - x_i) \in K[X]$ 为 E 在 K 上的 3-挠点多项式。四次多项式 ψ_3 有一个伽罗瓦预解式 $\delta_3 \in K[X]$，它是一个三次多项式，具有

$$\alpha_1 = x_1x_2 + x_3x_4, \qquad \alpha_2 = x_1x_3 + x_2x_4, \qquad \alpha_3 = x_1x_4 + x_2x_3$$

以其根为根。在 $\mathrm{GL}(U_3)/\langle -1\rangle = S_4$ 对 ψ_3的根的置换作用下，阶为 4 的正规子群 $V_4 \triangleleft S_4$ 固定这 3 个根 α_i。伽罗瓦群的两个自然满射

$$H_3 \to \mathrm{Gal}(\psi_3) \to \mathrm{Gal}(\delta_3) \tag{18}$$

是同构，因为它们是对适当子群限制后得到的泛群论映射

$$\mathrm{GL}(U_3) \to \mathrm{GL}(U_3)/\langle -1\rangle = S_4 \to S_4/V_4 = S_3.$$

更准确地说，(18) 中的第一个满射是单射，因为如 (17) 中所示，我们有 $-1 \notin H_3$ （对于 H_3 ）；第二个满射成立，是因为在 S_4中有 $\mathrm{Gal}(\psi_3) \cap V_4 = 1$：生成与矩阵第一列对应的伽罗瓦不变子空间的 3-扭点的 x坐标由 $\mathrm{Gal}(\psi_3)$固定。将 H_3 视为 $\mathrm{Gal}(\delta_3)$，我们可以引用一个经典公式 [13, p. 305] 来完成证明，该公式将 Δ_E 的三个立方根表示为 $b_4 - 3\alpha_i$ $(i = 1, 2, 3)$，其中 $b_i \in K$ 是来自 E的一个系数。这得到 $K(E[3]) = \mathrm{Split}_K(g) = \mathrm{Split}_K(X^3 - \Delta_E)$。□

由引理 6.1，可知对于（17）中的表示，子群 $\left(\begin{smallmatrix} 1 & * \\ 0 & 1 \end{smallmatrix}\right)$对应于扩张 $K(\zeta_3) \subset K(\zeta_3, \sqrt[3]{\Delta})$，其判别式值为 $\Delta = \Delta_{E'}$ 和 Δ_E。

我们可以将曲线 E' 写成德林标准形 [6, p。 89] 如下：

$$E' : y^2 + axy + by = x^3 \qquad \text{with } a, b \in K \text{ and } \Delta_{E'} = b^3(a^3 - 27b) \in K^*. \tag{19}$$

这里， $T = (0, 0) \in E'(K)$ 是三阶点，而商曲线 $E = E'/\langle T\rangle$的 Weierstrass 方程为

$$E : y^2 + axy + by = x^3 - 5abx - (a^3 + 7b)b, \tag{20}$$

3-同源 φ_3 的显式公式为： $E' \to E = E'/\langle T \rangle$

$$\varphi_3(x,y) = \left(\frac{x^3 + abx + b^2}{x^2}, \frac{y(x^3 - abx - 2b^2) - b(ax+b)^2}{x^3} \right). \tag{21}$$

由于 E 的判别式为 $\Delta_E = b(a^3 - 27b)^3$, , 当且仅当 $b \in K^*$ 是立方数且不等于 $(a/3)^3$时， K上的 3-除法域 $K(E[3])$ 等于 $K(\zeta_3)$。

若 a 非零，我们可以重新缩放（x， y） $\mapsto$ （a^2x， a^3y）并将（19）化简为

$$E'_b : y^2 + xy + by = x^3. \tag{22}$$

对于 K 一个数域，我们有无穷多个两两不同的 3-等ogeny 映像 $(E_b, P_b) = \varphi_3[(E'_b, P'_b)]$, 使得 $P_b \in E_b(K)$ 是非平凡的局部 3-非本原。

定理 6.2. 对于 K 一个数域，取 $b = b(X) = (1 - X - X^2)/X \in K(X)$，并将相应的椭圆曲线定义在 $K(X)$ 上，如下：

$$E_b : y^2 + xy + by = x^3 - 5bx - (1 + 7b)b.$$

于是，对无穷多个 $t \in K^*$， E_b 的特化 $E_{b(t)}$ 是定义在 K 上的一条椭圆曲线，对于该曲线，

$$\left(\frac{(t^2+t)(t^2-1)+1}{t^2}, \frac{(1-t^2)\left(t^4+2t^3+t-1\right)}{t^3} \right) \in E_{b(t)}(K) \tag{23}$$

是一个非平凡的局部 3-非原始点。

证明。 对于曲线 E'_b（22）中 $b \in K(X)$ 如上定义，点 $P'_b = (1, X)$ 位于 E'_b之上，这是由 b的选取方式决定的：它满足 $X^2 + X + bX = 1$。在 3-同源$\varphi_3 : E'_b \to E_b$ （21）从曲线映射到 E_b （将 $a = 1$ 代入（20）得到的曲线）的作用下，它被映射为

$$P_b = (1 + b + b^2, (1 - b - 2b^2)X - b(1+b)^2) \in E_b(K(X)).$$

在特化 $X = t \in K^*$下，我们得到点 $P_{b(t)}$，它位于曲线 $E_{b(t)}$上，该曲线定义在 K 上，由（23）给出。我们只关注使 $E_{b(t)}$ 成为椭圆曲线的那些特化。由于这些特化都满足 $t \in K^*$ 且 $b(t) \notin \{0, 1/27\}$，因此至多排除 4 个“坏”值 t 。此外，根据我们在 P_λ 的情形 $\ell = 2$下对 $t \in K^*$ 所作的同样论证，只有有限多个 P_t 会使其成为挠点。这些有限多个 t 也作为“坏”值排除。

我们已经看到， E_b 的3-除法域为 $K(\zeta_3, \sqrt[3]{b})$，而一项明确的计算表明，点 $P_b \in E_b(K(X))$的3-除法域等于

$$K(X)(\tfrac{1}{3}P_b) = K(\zeta_3, \sqrt[3]{b}, \sqrt[3]{X}) = K(\zeta_3, \sqrt[3]{X}, \sqrt[3]{X^2 + X - 1}).$$

在 $K(\zeta_3, X)$上，元素 X 和 $X^2 + X - 1$ 具有“独立”的立方根——只需考察它们的分歧轨迹即可。由此， P_b 在 $K(X)$ 上的 3-除法域的伽罗瓦群可描述为

$$\mathrm{Gal}(K(X)(\tfrac{1}{3}P_b)/K(X)) = \left\{ \begin{bmatrix} \omega_3 & x & y \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} : x, y \in \mathbf{F}_3 \right\},$$

其中 ω_3 表示对应于（可能是平凡的）扩张 $K(X) \subset K(X, \zeta_3)$ 的 $\mathbf{F}_3^*$-值特征。由希尔伯特不可约性可知，对于有限集‘坏’值之外的无穷多个 $t \in K^*$ ， 点 $P_{b(t)} \in E_{b(t)}(K)$ 的 3-除法域在 K 上具有‘相同的’伽罗瓦群，从而它成为一个全局 3-本原但局部 3-非本原的点。由于 $E_{b(t)}$ 不具有完整的

在 K 上的 3-挠，我们得出结论：点 $P_{b(t)}$ （见 23）是一个非平凡的局部 3-非本原点。□

注 6.3. 定理 6.2 证明中的构造排除了所有满足 $b = b(t) \in K^*$ 是立方数，且 (22) 中的椭圆曲线的 3-除法域为 $K(\zeta_3)$ 的特化。在这个特殊情形下，对于无穷多个 $b \in K^{*3}$，我们也可以为 $E = E_b$ 配备一个非平凡的局部 3-不可约点。我们先写出 $b = c^{-3}$，并将曲线在 $(x, y) \mapsto (c^{-2}x, c^{-3}y)$ 下变换为 E'：$y^2 + cxy + y = x^3$。与前一种情形一样，对于 $c = (-t^2 - t + 1)/t$，有 $P' = (1, t) \in E'(K)$，而 P' 在映射下的像是

$$\varphi : E' \to E = E'/\langle(0,0)\rangle : y^2 + cxy + y = x^3 - 5cx - (c^3 + 7)$$

是点 $P = \varphi_3(P') = ((-t^2 + t + 1)/t, (t^2 - 1)/t^2) \in E(K)$，其 3-除法域 $K(\frac{1}{3}P)$ 等于 $K(\zeta_3, \sqrt[3]{t})$。对于几乎所有 $t \notin K^{*3}$，这使 P变成一个全局 3-本原点，同时也是局部 3-非本原点。

我们结束关于 $\ell = 3$ 的讨论，其中剩余的情形是，(19)中的曲线E' 具有 $a = 0$。在此情形下，E' 具有 j-不变量0，并令 $c = b/2$，我们可以通过 $y \mapsto y - c$ 将方程缩放为更熟悉的形式 E'：$y^2 = x^3 + c^2$，其中有3-扭点 $T = (0, c)$，并且具有由 $\mathbb{Z}[\zeta_3]$给出的复乘。我们通过令 $c = s^2 - 1$ 且 $s \in K$，为 E' 配备一个 K-有理点 $(c, c\sqrt{c+1})$。这导出一个单参数族的 3-同源

$$\varphi_3 : E'_s : y^2 = x^3 + (s^2 - 1)^2 \longrightarrow E_s : y^2 = x^3 - 27(s^2 - 1)^2$$
$$P'_s = (s^2 - 1, s(s^2 - 1)) \longmapsto P_s = (s^2 + 3, s(s^2 - 9))$$

在具有 j-不变量0的复乘曲线之间。在这种情况下，E_s 在 K上的 3-除法域是 $K(\zeta_3, \sqrt[3]{2(s^2 - 1)})$，而 P_s 在 K 上的 3-除法域等于

$$K(\zeta_3, \sqrt[3]{2(s^2 - 1)}, \sqrt[3]{4(s + 1)}).$$

同样，对于薄集之外的 $s \in K$，点 $P_s \in E_s(K)$ 是全局 3-本原的，但局部 3-非本原。

7. 更多示例

在 $K =$ 有理数域上，非平凡的局部非本原点只能出现在素数$\ell \le 7$中。关于 $\ell = 5$ 以及 $\ell = 7$ 的例子可以通过我们用于 $\ell = 3$的技术找到，但公式和所得的曲线很快就变得不太适合在纸面上展示。

7.1. 具有局部 5-非本原点的曲线。在这种情况下，我们从 m
Tate 标准形式

$$E' : y^2 + (1 - c)xy - cy = x^3 - cx^2 \tag{24}$$

该参数化了以 (0,0) 为 5-有理点的椭圆曲线（见 Kulesz [7]）。它还有 $(0, c)$、$(c, 0)$ 和 (c, c^2) 这些 5 阶点，其判别式等于$\Delta_{E'} = c^5\,(c^2 - 11c - 1)$。利用 V´élu 公式 [18] 或调用 Pari-GP，我们计算出 5-同源曲线的 Weierstrass 方程 $E = E'/\langle(0,0)\rangle$

$$E = E_c : \quad y^2 + (1 - c)xy - cy = x^3 - cx^2 - 5c(c^2 + 2c - 1)x - c(c^4 + 10c^3 - 5c^2 + 15c - 1),$$

以及显式的 5-同源 $\varphi_5: E' \to E$。涉及的判别式为$\Delta_{E'} = c^5(c^2-11c-1)$和 $\Delta_E = c(c^2-11c-1)^5$,，与我们在 $\ell=3$中看到的情形非常相似。 E' 和 E 的 5-挠表示如（17）所示；尽管引理 6.1 对于 $\ell=3$ 的证明不能推广到 $\ell=5$，但我们通过直接计算发现，5-除法域为 $K(E'[5]) = K(\zeta_5, \sqrt[5]{c^2-11c-1})$ 以及$K(E[5]) = K(\zeta_5, \sqrt[5]{c})$：它们是在 $K(\zeta_5)$ 上由判别式的 5 次方根生成的。

我们可以为 E' 配备一个 K-有理点 $P'_t = (t,t)$，通过令 $c = t(2-t)$，并将其像 $P_t = \varphi_5(P') \in E_{t(2-t)}(K)$ 计算为

$$P_t = \left(\tfrac{2t^4-8t^3+11t^2-6t+2}{(t-1)^2}, -\tfrac{t^8-7t^7+19t^6-23t^5+4t^4+23t^3-31t^2+19t-4}{(t-1)^3}\right).$$

与 P_t 对应的 5-除法域是

$$K(\tfrac{1}{5}P_t) = K(\zeta_5, \sqrt[5]{t}, \sqrt[5]{t-2}).$$

如果这是 $K(\zeta_5, \sqrt[5]{c}) = K(\zeta_5, \sqrt[5]{t(t-2)})$ 的次数为5的扩张，那么 P_t 是 $E_{t(2-t)}(K)$ 中一个全局 5-本原但局部 5-非本原点。

例 7.1。取 $K=$ 有理数域。对于 $t=1$，上面的点 P_t 是零点，因为 P'_t是 5-挠；对于 $t=2$，我们有 $c=0$，且 E 是奇异的；而对于 $t=3$ 和 4，我们遇到了“意外” $t=-c$ 和 $tc=2^5$，从而得到点 $P_t \in 5E_{t(2-t)}(\mathbb{Q})$。对于 $t=5$，我们得到点 $P_5 = (497/16, -73441/64)$ 在上面。

$$E_{-15}: y^2+16xy+15y = x^3+15x^2+14550x+232860,$$

它是 LMFDB 数据库中的曲线 5835.c2。注意，对于 $c=-15$，我们有

$$c(c^2-11c-1) = -5835 = -3\cdot 5\cdot 389.$$

局部 5-非本原点 P_5 是 $E_{-15}(\mathbb{Q}) \cong \mathbb{Z}$ 的生成元。事实上，对于所有不是五次幂或加 2 后为五次幂的 $t \in \mathbb{Z}_{\geq 5}$，$P_t$ 在 $E_{t(2-t)}(\mathbb{Q})$ 中都是全局 5-本原但局部 5-非本原的，因为对于这些 t，由 t 和 $t-2$ 生成的 $\mathbb{Q}^*/\mathbb{Q}^{*5}$ 子群的阶为 25。

7.2. 具有局部 7-非本原点的曲线。我们仍从 Tate 正规方程出发

$$E': y^2+(1-c)xy-by = x^3-bx^2$$

但现在我们不施加 $b=c$，如同对 $\ell=5$ 的情形，而是改为

$$c = d^2-d \quad \text{and } b = d^3-d^2.$$

曲线 $E' = E'_d$ 参数化 [7] 以 (0，0) 为 7阶点的椭圆曲线。7-同源曲线 $E = E'/\langle\langle(0,\ 0)\rangle\rangle$ 的 Weierstrass 方程为

$$\begin{aligned} E: y^2+(1-c)xy-by = x^3-bx^2 &- 5\left(2b^2+b\left(c^2-3c-2\right)+c\left(c^2+4c+1\right)\right)x \\ &-b^2\left(12c^2+c+24\right)-6b^3+b\left(-c^4+9c^3+46c^2+24c+2\right)- \\ &c\left(c^4+16c^3+36c^2+16c+1\right). \end{aligned}$$

其判别式为 $\Delta_E = d(d-1)(d^3-8d^2+5d+1)^7$,，这次我们发现其7-等分域为 $K(E[7]) = K(\zeta_7, \sqrt[7]{d(d-1)^2})$。

通过令 $d=d(t) = (t+1)/(t^2-t+1)$，我们赋予 E' 一个 K-有理点 $P'_t = (d^2t, d^3t)$。P'_t 在 7-同源 $E' \to E$ 下的像为

$$P_t = \left(-\frac{C(t)}{(2t-1)^2(t-1)^2\left(t^2-t+1\right)^4}, \frac{D(t)}{(t-1)^3(2t-1)^3\left(t^2-t+1\right)^6}\right) \in E(K)$$

其中 $C(t)$ 和 $D(t)$ 是 $\mathbf{Z}[t]$ 中次数分别为 12 和 18 的某些多项式。用 t 表示，7-等分域为 $K(E[7]) = K(\zeta_7, \sqrt[7]{t^2(t+1)(t-2)^2(t^2-t+1)^4})$，而 P_t 的 7-等分域为

$$K(\tfrac{1}{7}P_t) = K(E[7])\left(\sqrt[7]{\tfrac{t(t+1)}{t-2}}\right) = K\left(\zeta_7, \sqrt[7]{\tfrac{t(t^2-t+1)}{(t+1)}}, \sqrt[7]{\tfrac{t(t+1)}{(t-2)}}\right).$$

点 P_t 是全局 7-本原但局部 7-非本原的点，当扩张 $K(\zeta_7) \subset K(\frac{1}{7}P_t)$ 的一般次数为 7^2 时。

例 7.2。取 $K =$ 有理数域。对于 $t = 1$，上面的点 P_t 是零点，因为 P_t' 是 7-挠点；对于 $t = 2$，曲线 E' 是奇异的。然而，对于 $t = 3$ 和 $d = \frac{4}{7}$，我们得到点 $P_3 = (286019/490^2, 15951227/490^3)$，位于

$$E : y^2 + \tfrac{61}{7^2}xy + \tfrac{48}{7^3}y = x^3 + \tfrac{48}{7^3}x^2 - \tfrac{774780}{7^7}x - \tfrac{1047829260}{7^{11}},$$

即为具有最小模型的曲线 20622.j1

$$E_0 : y^2 + xy = x^3 - 5455771x - 5039899603,$$

在 LMFDB 数据库中。我们的局部 7-不可约点 P_3 是E(有理数域) $\cong \mathbf{Z}$ 的生成元。在 E_0 上，对应的生成元是 $(328219/10^2, 109777927/10^3)$。

8. A composite level obstruction

到目前为止，我们一直关注素数层级 ℓ上局部本原性的非平凡阻碍，因为这是椭圆曲线本原根情形 III 中一种新现象，在乘法原根情形 I 和循环约化情形 II 中并不会出现。

在这三种情形中，复合层上还存在性质各异的阻碍，这些阻碍源于有限多个相应除法域 K_ℓ之间的纠缠。这些阻碍不会在 $K =$有理数域上出现；情形 I 和 II 中的大多数例子，都是通过基变换到定义域有理数域 $\mathbf{Q}(x)$ 和 $\mathbf{Q}(j_E)$ 的某个精心选取的有限扩张而产生的。这里情形 III 也有所不同，因为纠缠阻碍在有理数域 $\mathbf{Q}$ 上就已出现。本节构造一个 6 层障碍。

设 E/K 是一个椭圆曲线，且 $\#E[2](K) = 2$，并且 $P \in E(K)$ 是一个无限阶点。那么，2-除法域 $K(E[2](\overline{K}))$ 是K的二次扩张。假设 $K(\frac{1}{2}P)$ 的 2-除法域 P 在其上的次数为最大次数 4。那么 $G_2 = \mathrm{Gal}(K(\frac{1}{2}P)/K)$ 是一个阶为 8 的二面体群，其在 6 上的矩阵表示（$V_2 = \langle \frac{1}{2}P\rangle/\langle P\rangle$）具有如下形式

$$G_2 = \left\{ \begin{bmatrix} 1 & a & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{bmatrix} : a, b, c \in \mathbf{F}_2 \right\} \subset \mathrm{GL}_3(\mathbf{F}_2). \tag{25}$$

存在一个唯一子域 $L \subset K(\frac{1}{2}P)$，其在 K上的伽罗瓦群同构于克莱因四元群 $V_4 = C_2 \times C_2$；我们可以将 a 和 b 视为 25 的矩阵表示 G_2 中的 $\mathbf{F}_2$-值二次特征，它们生成 G_2 的商群伽罗瓦群$(L/K) \cong V_4$ 的特征群，该商群是 G_2的商群。

对于素数 $\mathfrak{p} \nmid 2\Delta_E$，点 P 在 $E(k_\mathfrak{p})$ 中生成奇数指数子群，当且仅当其弗罗贝尼乌斯 $\mathrm{Frob}_{\mathfrak{p},\,2} \in G_2$如（25）中所示视为矩阵时，自同态 $(\mathrm{Frob}_{\mathfrak{p},\,2} - \mathrm{id}_2)$: $V_2 \to V_2$ 的 $\mathbf{F}_2$-秩至少为 2（引理 2.3）。由此得到判据

$$2 \nmid [E(k_\mathfrak{p}) : \langle \overline{P}\rangle] \iff a(\mathrm{Frob}_{\mathfrak{p},2}) = b(\mathrm{Frob}_{\mathfrak{p},2}) = 1 \in \mathbf{F}_2. \tag{26}$$

更确切地说， $a(\mathrm{Frob}_{\mathfrak{p},2}) = 1$ 意味着 $E(k_{\mathfrak{p}})$ 不具有完整的 2-扭点，并且$b(\mathrm{Frob}_{\mathfrak{p},\ 2}) = 1$ 意味着 P 不仅不在 $2E(k_{\mathfrak{p}})$ 中，而且也不是定理 1.2条件 C 中所述的 2-同源像。

进一步假设 E 有一个 K-有理的 3-扭子群 T，并设 $\varphi_3 : E' \to E$ 是与商映射 $\phi : E \to E' = E/T$ 对偶的同源。假设点 P属于 $\varphi_3[E'(K)]$，但不属于 $3E(K)$。那么， P的 3-除法域 $K(\frac{1}{3}P)$ 的伽罗瓦群为 $G_3 = \mathrm{Gal}(K(\frac{1}{3}P)/K)$；其在 $V_3 = \langle \frac{1}{3}P\rangle/\langle P\rangle$ 上的矩阵表示「通常」是如下的群：

$$G_3 = \left\{ \begin{bmatrix} d & e & f \\ 0 & g & 0 \\ 0 & 0 & 1 \end{bmatrix} : \quad d, g \in \mathbf{F}_3^*, e, f \in \mathbf{F}_3 \right\} \subset \mathrm{GL}_3(\mathbf{F}_3) \tag{27}$$

阶为36。在这种情况下， d 和 g 可以看作二次特征 $G_3 \to \mathbf{F}_3^*$，再应用引理2.3 可知，对于素数 $\mathfrak{p} \nmid 3\Delta_E$，有

$$g(\mathrm{Frob}_{\mathfrak{p},3}) = 1 \in \mathbf{F}_3^* \quad \Longrightarrow \quad 3 | [E(k_{\mathfrak{p}}) : \langle \overline{P}\rangle]. \tag{28}$$

因此，对于素数 $\mathfrak{p} \nmid 6\Delta_E$，要使 $\overline{P} \in E(k_{\mathfrak{p}}$成为椭圆曲线本原根，一个必要条件是三个二次特征 a、 b 和 g （见式26）和式28）中出现的那些特征在 $\mathfrak{p}$中的弗罗贝尼乌斯自同构下均不为零。 $K_6 = K(\frac{1}{6}P$换言之，素数 $\mathfrak{p}$ 必须在与这三个特征对应的二次扩张 K_a、 K_b 和K_g 中 K 保持惰性。

满足上述条件的素数 $\mathfrak{p}$ 存在，当二次扩张 K_a、K_b 和 K_g 在 K 上线性互不相交时；但若它们是一个 V_4-扩张 $K \subset K_aK_bK_g$ 的三个二次子域，则不存在。在后一种情形中，对于 K_6 中的 P 的局部本原性，存在一种分裂障碍，而在较小的域 $K(\frac{1}{2}P)$ 或 $K(\frac{1}{3}P)$ 中则不存在：该障碍的层级为 6，而非 2 或 3，因此是由除法域纠缠所导致的。

例 8.1。一个例子是 LMFDB 数据库中标签为 12100.j1 的椭圆曲线 $E/\mathbf{Q}$。该曲线 E 的判别式为

$$\Delta_E = 2^4 \cdot 5^9 \cdot 11^6,$$

若取 (0, 0) 为其唯一的有理数域 Q-有理 2-扭点，则它的魏尔斯特拉斯模型为

$$E : y^2 = x^3 + 605x^2 - 3025x.$$

对于这条曲线，我们有 $E(\mathbf{Q}) = \langle T_2\rangle \times \langle P\rangle \cong \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}$，其中 $T_2 = (0, 0)$ 的阶为 2，而 $P = (\frac{-13475}{36}, \frac{1249325}{216})$ 是一个无穷阶生成元。我们有 $K_a = \mathbf{Q}(E[2]) = \mathbf{Q}(\sqrt{\Delta_E}) = \mathbf{Q}(\sqrt{5})$，在这个域上， P 的 2-除法域 $\mathbf{Q}(\frac{1}{2}P)$ 是 V_4扩张

$$\mathbf{Q}(E[2]) = \mathbf{Q}(\sqrt{5}) \subset \mathbf{Q}(\tfrac{1}{2}P) = \mathbf{Q}(\sqrt{5}, \sqrt{\pi}, \sqrt{\overline{\pi}})$$

由 $\pi = 3 + 2\sqrt{5}$ 及其共轭元的平方根生成。由 $\pi\overline{\pi} = -11$可知，有理数域$(\frac{1}{2}P)$是有理数域$(\sqrt{-55})$上的 4 次循环扩张，并且我们有 K_b =有理数域$(\sqrt{-11})$。

由于 E 在二次域 $\mathbf{Q}(\sqrt{165}) = \mathbf{Q}(\sqrt{-3 \cdot -55})$ 上获得了一个 3-扭点 $T_3 = (55\ 3$, $\frac{275}{9}\sqrt{165})$，该扭点生成了一个阶为3的定义在有理数域上的扭子群，因此 E 的 3-除法域具有二次子域 $K_d = \mathbf{Q}(\sqrt{165})$ 和 $K_g = \mathbf{Q}(\sqrt{-55})$，

使 K_g 成为 V_4-扩张 $\mathbb{Q} \subset K_a K_b$ 中的第三个二次子域。在 E的完整 3-除法域上， P 的 3-除法域是三次扩张

$$\mathbf{Q}(E[3]) = \mathbf{Q}(\sqrt{-3}, \sqrt{-55}, \sqrt[3]{2}) \subset \mathbf{Q}(\tfrac{1}{3}P) = \mathbf{Q}(E[3], \sqrt[3]{\alpha})$$

由某个元素的立方根生成 $\alpha = (3+\sqrt{-55})/2 \in K_g$，其范数为 16。这表明它在 有理数域 上的伽罗瓦群是 G_3 （27）中的群。因此我们得出， P是 E(有理数域) 上的局部处处非本原点，因为 $\langle \overline{P} \rangle$ 在 $E(\mathbf{F}_p)$ 中的指数总是能被 2 或 3 整除。

一篇即将发表的论文将进一步讨论复合层级下本原性的阻碍，并介绍如何找到具体实例。

References

[1] George Cooke 和 Peter J. Weinberger, *On the construction of division chains in algebraic number rings with applications to* $_2$, **3** 1975 481 524 , SL《Communications in Algebra》（），–。[2] Francesco Campagna 和 Peter Stevenhagen, *Cyclic reduction densities for elliptic curves*, arXiv 预印本 2001.00028，已投稿。[3] Rajiv Gupta 和 M. Ram Murty, *Cyclicity and generation of points mod p on elliptic curves*, 《Inventiones Mathematicae》101（1990），第 1 期，225–235。[4] , *Primitive points on elliptic curves*, 《Compositio Mathematica》58（1986），第 1 期，13–44。[5] Christopher Hooley, *On Artin's conjecture*, 《Journal für die reine und angewandte Mathematik》225（1967年），209–220。[6] Dale Husem¨oller, *Elliptic curves, 2nd edition*, 施普林格出版社，纽约，2004年。[7] Leopoldo Kulesz, *Families of elliptic curves of high rank with nontrivial torsion group over* 有理数域, 《Acta Arithmetica》108（2003），第 4 期，339–356。[8] Serge Lang 和 Hale Trotter, *Primitive points on elliptic curves*, 《Bulletin of the American Mathematical Society》83（1977），第 2 期，289–292。[9] H. W. Lenstra Jr., *On Artin's conjecture and Euclid's algorithm in global fields*, 《Inventiones Mathematicae》42（1977），201–224。[10] H. W. Lenstra Jr.、P. Stevenhagen 和 P. Moree, *Character sums for primitive root densities*, 《Mathematical Proceedings of the Cambridge Philosophical Society》157（2014），第 3 期，489–511。[11] Giulio Meleleo, *Questions related to Primitive Points on Elliptic Curves and Statistics for Biquadratic Curves over Finite Fields* ` 2015 ，博士论文，罗马第三大学（）。[12] Lo¨ıc Merel, *Bornes pour la torsion des courbes elliptiques sur les corps de nombres*, 《Inventiones Mathematicae》124（1996），第 1–3 期，437–449（法语）。[13] Jean-Pierre Serre, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*, 《Inventiones Mathematicae》15（1972），第 4 期，259–331。[14] , *Abelian ℓ-adic representations and elliptic curves*, Benjamin，纽约，1968年。[15] , *Résumé des cours de 1977-1978*, Springer 数学文集，施普林格出版社，海德堡，2013年。1986年原版的2003年版重印本 [，MR0926691]。[16] Peter Stevenhagen 和 Hendrik Lenstra, *Chebotarev and his density theorem*, 《Mathematical Intelligencer》18（1996），第 2 期，26–37。[17] Peter Stevenhagen, *The correction factor in Artin's primitive root conjecture*, 《J. Th´eor. Nom-bres Bordeaux》15（2003），第 1 期，383–391（英语，附英语和法语摘要）。第二十二届算术会议（里尔，2001年）。[18] Jacques V´elu, *Isogénies entre courbes elliptiques*, 《巴黎科学院报告》S´ér. A-B 273（1971），A238–A241（法语）。

Department of Mathematics, Statistics and Computer Science, University of Illinois at Chicago, 851 S Morgan St, 322 SEO, Chicago, IL 60607, USA

Dipartimento di Matematica, Università Roma Tre, Largo S. L. Murialdo 1, I–00146 Rome, Italy

Mathematisch Instituut, Universiteit Leiden, Postbus 9512, 2300 RA Leiden, The Netherlands*Email address*: ncjones@uic.edu, pappa@mat.uniroma3.it, psh@math.leidenuniv.nl