arXiv:2611.32749v1 [math.NT] 24 Nov 2026

超奇异素数处指数为一的椭圆 Lehmer 界

JORGE MELLO

Abstract. 设 E 是定义在数域 K 上的一条椭圆曲线，并且在素数 $\mathfrak{p}$处具有良好超奇异约化。我们证明，每个非挠 $P \in E(K)$ 的 N´éron–Tate 高度都满足$\widehat{h}_E(P) \geq c\,D^{-1}(\log 3D)^{-1}\exp(-c'\sqrt{\log 3D})$，其中 $D = [K(x(P)) : K]$ 以及 $c,\ c' > 0$ 仅取决于 E、 K 和 $\mathfrak{p}$；因此 $\widehat{h}_E(P) \geq D^{-1-o(1)}$。根据 Elkies 的一个结果，这适用于定义在 $\mathbb{Q}$上的每条椭圆曲线，并改进了 Masser 以及 Hindry 和 Silverman 的指数。

1. Introduction

设 E 是数域 K 上的一条椭圆曲线，并记 h_E 其 N´éron–Tate 高度。对于次数为 $D = [K(P) : K]$ 的非挠点 P，椭圆 Lehmer 问题询问是否有 $h_E(P) \geq c(E)/D$。对于具有复乘的曲线，Laurent [12] 利用许多分裂素数处的 Frobenius 端同态证明了 Dobrowolski 型界 $c\,D^{-1}(\log\log 3D/\log 3D)^3$,。对于具有非整数 j-不变量的曲线，Hindry 和 Silverman [9] 证明了$c/(D^2\log^2 3D)$；而对于所有曲线，Masser [13] 证明了 $c/(D^3\log^2 3D)$；对于整数 j-不变量且不具有复乘的情形，据我们所知，这曾是最佳指数。

在全文中， K 是一个数域， K 中位于有理素数 p 之上的一个素数为 $\mathfrak{p}$，其分歧指数为 e，剩余次数为 f。令 $\mathcal{O} = \mathcal{O}_{K,\mathfrak{p}}$ 为局部环， $k = \mathcal{O}/\mathfrak{p}$ 且 $N\mathfrak{p} = p^f$。设 E/K 由一个系数属于 $\mathcal{O}$ 且判别式属于$\backsim\mathcal{O}^\times$ 的魏尔斯特拉斯方程给出，其约化 E 为超奇异的；每条在 $\mathfrak{p}$ 处具有良好超奇异约化的椭圆曲线都有这样的方程。对于 $P \in E(K)$，令 $e_{\mathfrak{p}}(P)$ 表示 $K(P)$ 中位于 $\mathfrak{p}$ 之上的素数的最大绝对分歧指数，从而 $e_{\mathfrak{p}}(P) \leq e[K(P) : K]$。

我们的主要结果是：对于每条具有良好超奇异约化素数的曲线，都有一个指数为 $1 + o(1)$ 的下界。对于所有此类曲线，它改进了 Masser 的指数 3；当$j(E)$ 不是整数时，也改进了 Hindry 和 Silverman 的指数 2。

定理 A。 存在仅取决于 E、 K 和 $\mathfrak{p}$ 的 c_1、 $c_2 > 0$，使得每个非挠$P \in E(K)$ 均满足：当 $D = [K(x(P)) : K]$ 时：

(i) $$\widehat{h}_E(P) \geq \frac{c_1}{e_{\mathfrak{p}}(P)\,D}\exp\bigl(-c_2\sqrt{\log 3D}\bigr);$$

(ii) $$\widehat{h}_E(P) \geq \frac{c_1}{D\log 3D}\exp\bigl(-c_2\sqrt{\log 3D}\bigr).$$

特别地 $\widehat{h}_E(P) \geq D^{-1-o(1)}$ 对所有非挠 P均成立。

Date：工作笔记，2026年11月。

根据 Elkies 的一项结果，该假设对 $\mathbb{Q}$ 上的每条椭圆曲线都成立，更一般地，在以下情形中也成立。

推论 1.1。设 E 是定义在 $\mathbb{Q}$上的一条椭圆曲线，或更一般地，设其定义在数域K 上，且 E 具有复乘，或者 $\mathbb{Q}(j(E))$ 具有实嵌入。则存在仅依赖于 E 和 K的c、$c'>0$，使得每个非挠 $P\in E(K)$ 都满足：当$D=[K(x(P)):K]$,

$$\widehat{h}_E(P) \;\geq\; \frac{c}{D\log 3D}\exp\bigl(-c'\sqrt{\log 3D}\bigr);$$

特别地，$\widehat{h}_E(P) \geq D^{-1-o(1)}$。

证明。这样的曲线具有一个良好超奇异约化素数：在 $\mathbb{Q}$ 由 Elkies 给出 [6], ，一般情形则由命题 11.1给出。应用定理 A。□

由于 $[K(x(P)):K]\leq[K(P):K]$，且下界随 D 增大而减小，因此它们在$D=[K(P):K]$时同样成立，并且指数 1 是最优的：如果 Q 在 K的有限扩张K'上是非挠的，且 $[m]P=Q$，那么 $[K(P):K]\leq m^2[K':K]$，以及 $\widehat{h}_E(P)=\widehat{h}_E(Q)/m^2$（另见注 10.4）。对于具有复乘的曲线，Laurent 界更强。当 $e_{\mathfrak{p}}(P)<\log 3D$ 时，部分 (i) 给出的下界更优。

在这里，除其他内容外，我们将 Dobrowolski 方法应用于单个素数；该方法通常对许多素数 p 使用同余 $A(x^p)\equiv A(x)^p$ (模 p)。令 φ 为 $[p]$ 的 Latt`es 映射，即次数为 p^2 的有理映射，并且对所有 $Q\in E$ 都有 $x([p]Q)=\varphi(x(Q))$。其模 $\mathfrak{p}$ 的约化为 $x\mapsto(x^{p^2}+s)/c$，其中 $c\neq 0$ 和 s 满足相应条件（引理 7.2）；由此我们推出，零点为 $\alpha_n=x([p^n]P)$ 的共轭元的二元形式 A_n 对固定的 $q\geq 1$ 满足 $A_{n+q}\equiv\pm A_n$ （模 $\mathfrak{p}^{n+1}$）（定理 5.2）。这与 Baker 对 φ 的动力 Green 函数能量所给出的下界相结合；也就是说，对沿轨道经过 $\asymp\sqrt{\log D}$ 个连续步骤的点对，将 φ 的 Green 函数求和。记 $D_n=[K(\alpha_n):K]$ 和 $r_n=D_n/D_{n+1}\in\{1,\dots,p^2\}$；当 $r_n\geq 2$ 时，第 n 步出现次数下降。我们得到如下结果。

定理。存在 c、$c'>0$ 和 $k(D)=O(\sqrt{\log 3D})$，使得每个非挠 $P\in E(K)$ 都满足以下条件：如果 D_n 对 $m\leq n\leq m+k(D_m)$ 为常数，那么

$$\widehat{h}_E(P) \;\geq\; \frac{c}{D}\exp\bigl(-c'\sqrt{\log 3D}\bigr)\prod_{n<m}\frac{r_n}{p^2}.$$

这是定理2.1应用于拉泰`映射，根据引理7.3。令 $m=0$它给出$\widehat{h}_E(P)\geq c\,D^{-1}\exp(-c'\sqrt{\log 3D})$，只要在最初的 $k(D)$ 步中次数不下降，例如当 D 的每个素因子都 p^2大于 r_n 时，因为每个$[1,p^2]$ 都是整除 D的整数。一般而言，每一步 $n<m$ 带有 $r_n<p^2$ 都会使下界降低因子r_n/p^2，因此需要控制次数下降发生的位置。

为此，我们研究 φ 在 $\mathfrak{p}$上的动力学。点 z 若是周期的，则 $\varphi^n(z)=z$ 对某个$n\geq 1$成立；若是临界的，则 φ 在 z附近不是单射；Latt`ès 映射没有周期临界点（引理7.4）。$\mathbb{P}^1(\mathbb{C}_p$的每个剩余圆盘，即模 $\mathfrak{p}$约化相同的点集，

恰好包含一个周期点。如果在步骤 n 处次数下降，则 α_n 的两个共轭元在 φ 下具有相同的像。如果二者都位于 $x(P)$ 的共轭元之上，且这些共轭元在 $K_{\mathfrak{p}}$ 上的域具有较小的分歧指数，那么它们在 $\mathfrak{p}$-进意义下都接近其剩余圆盘的周期点 η，而差商表明，φ 在 η 处的导数具有较大的 $\mathfrak{p}$-进赋值。这是不可能的，因为该赋值在周期点上有界，而周期点中没有一个是临界点。对 φ 的每个纤维应用这一结论，我们得到：步骤 m 处的次数下降迫使 $x(P)$ 的至少一半共轭元在 $\mathfrak{p}$ 上方具有分歧指数 $\gg p^{2m}$（引理 9.3）。取 m 为最后一次次数下降，即得 (i) 部分。对于 (ii) 部分，我们利用这些分歧的共轭元形成 $\mathfrak{p}$-进簇，即由 $\asymp e_{\mathfrak{p}}(P)$ 个两两在 $\mathfrak{p}$-进意义下接近的共轭元组成的集合，因此 α_m 的共轭元在 $\mathfrak{p}$ 处具有较大的能量，也就是说，它们两两之间 $\mathfrak{p}$-进弦距离的 $-$ 对数之和较大（命题 9.5）。这给出 $\widehat{h}_E(P) \gg D^{-1}$，除非 $D_m p^{2m} \ll D \log D$；在后一种情况下，将上述下界应用于最后一次次数下降之后，即得 $\widehat{h}_E(P) \gg (D_m p^{2m})^{-1} \exp(-c'\sqrt{\log 3D})$。

作为局部分析的一个副产品，当 $\mathfrak{p}$ 之上的剩余次数有界时，我们得到一个仅依赖于分歧的下界：定理A 中的因子 $\exp(-c_2\sqrt{\log 3D})$ 和 $\log 3D$ 消失，而对分歧的依赖是尖锐的。

定理 B. 设 $f_0 \geq 1$。存在一个仅依赖于 E、K、$\mathfrak{p}$ 和 f_0 的 $c_3 > 0$，使得每个非挠 $P \in E(K)$，只要 (P) 中每个位于 $\mathfrak{p}$ 之上的素数的绝对剩余次数至多为 f_0，就满足

$$\widehat{h}_E(P) \;\geq\; \frac{c_3}{e_{\mathfrak{p}}(P)} \;\geq\; \frac{c_3}{2e\,D}, \qquad D = [K(x(P)) : K].$$

特别地，如果 $\mathfrak{p}$ 之上的分歧也有界，那么 $h_E(P)$ 有一个正的下界。

(P) 的指数无法降低（注10.4）。证明（§10）比较轨道中一对相邻层次；它利用 $[p]$ 在每个剩余 $\mathfrak{p}$类（约化映射的纤维 $E(\mathbb{C}_p) \to E(\mathbb{F}_p)$）附近按 $\mathfrak{p}$-进方式压缩形式群，并且 P 的共轭元落在有界多个剩余类中。对于 Weil 高度，Bombieri 和 Zannier [3] 在局部次数有界的域上给出了下界，其中分歧指数以相同方式起作用；Baker 和 Petsche [2] 证明了椭圆曲线在全体p-进域上具有 Bogomolov 性质。

我们在表1 中以 $h_E(P) \geq D^{-\ell-o(1)}$的形式总结了上述下界以及我们的下界，其中 $D = [K(P) : K]$ 并且 $o(1)$ 表示一个当 $D \to \infty$ 趋于 0 且仅取决于 E的量，K（以及 $\mathfrak{p}$，f_0）。

本文证明的一些结果也可用于改进阿贝尔簇的相关结论。设 A 是定义在 K 上、维数为 g 的阿贝尔簇，$\mathcal{L}$ 是 A上的丰对称线丛，和 h_A，$\mathcal{L}$ 表示 Néron–Tate 高度。对于次数为 $D = [K(P) : K]$ 的非挠 $P \in A(K)$，Masser 证明了 $\widehat{h}_A(P) \geq c\,D^{-(2g+1)}(\log 3D)^{-2g}$ [14, 8]。最后，我们从定理 A 推导出，对于与椭圆曲线乘积同源的阿贝尔簇，指数为 $1 + o(1)$，取代了 Masser 的 $2g + 1$。

下界适用于 $\widehat{h}_E(P)$	对 E/K 或 P的限制	参考文献
$D^{-1-o(1)}$	E 具有复乘	Laurent 1983 [12]
$D^{-3-o(1)}$	none	Masser 1989 [13]
$D^{-2-o(1)}$	$j(E)$ 非整数	Hindry–Silverman 1990 [9]
$D^{-1-o(1)}$	E 有一个良好超奇异约化素数（例如每个 $E/\mathbb{Q}$）	定理 A
$c\,e_{\mathfrak{p}}(P)^{-1} \geq c(2eD)^{-1}$	E 在 $\mathfrak{p}$处超奇异，剩余次数 $K(P)$在 $\mathfrak{p}$ 上方的 f_0至多为 f_0	定理 B

TABLE 1. 椭圆 Lehmer 问题中的下界。

定理 C. 设 K'/K 是一个有限扩张，并假设 $A_{K'}$ 在 K' 上与 K'上椭圆曲线的乘积 $E_1 \times \cdots \times E_g$ 同源，且其中每条椭圆曲线都有一个良好超奇异约化素数。那么存在 c、$c' > 0$，它们仅取决于 A、$\mathcal{L}$、K' 和该同源，使得每个非挠 $P \in A(K)$ 都满足

$$\widehat{h}_{A,\mathcal{L}}(P) \;\geq\; \frac{c}{D \log 3D} \exp\bigl(-c'\sqrt{\log 3D}\bigr), \qquad D = [K(P) : K].$$

该假设适用于定义在 $\mathbb{Q}$ 上且同源于 $\mathbb{Q}$ 的任意阿贝尔簇乘积，其中各因子均为椭圆曲线；也适用于具有复乘或具有$\mathbb{Q}(j(E))$且拥有一个实嵌入的椭圆曲线的魏尔限制，其中一些在 $\mathbb{Q}$ 上是12.2的推论。

在第 2–6 节中，我们证明有理映射次数为 p^2 、在仿射变量变换下提升 p^2 次弗罗贝尼乌斯的窗口界，全程不使用椭圆曲线。第7 节介绍关于 ` 上的拉泰映射 $[p]$ 的必要背景，第 8 节讨论其在$\mathfrak{p}$处的动力学。定理 A 在 §9 中证明，定理 B 在 §10 中证明，定理 C在 §12 中证明，而§11 节讨论超奇异素数。

2. 提升弗罗贝尼乌斯的映射

本节固定一个次数为 p^2 的有理映射，其在 $\mathfrak{p}$ 处的约化是弗罗贝尼乌斯后接一个仿射映射，并陈述该映射的窗口界；此界将在§§3–6中证明。

设 K、$\mathfrak{p}$、p、e、f、$\mathcal{O}$ 和 k 如引言中所述，并令 $d = p^2$。在 §§2–6 中，我们固定一对$\Phi = (\Phi_0, \Phi_1)$次数为 d 、系数属于 $\mathcal{O}$的二元形式，以及元素 $c \in \mathcal{O}^\times$、$s \in \mathcal{O}$，使得

$$\Phi \;\equiv\; \Psi \pmod{\mathfrak{p}}, \qquad \Psi = \bigl(X^d + sZ^d,\; cZ^d\bigr), \tag{1}$$

该同余按系数逐项成立。结式 $\mathrm{Res}(\Phi) = \mathrm{Res}(\Phi_0, \Phi_1)$ 是 $\mathcal{O}$ 中的一个单位元，因为其约化为 $\mathrm{Res}(X^d + sZ^d, cZ^d) = \pm c^d \neq 0$。因此，$\Phi_0, \Phi_1$ 在 $\mathbb{P}^1(K)$ 中没有公共零点，而 Φ 定义了一个有理映射 $\varphi\colon \mathbb{P}^1 \to \mathbb{P}^1$，其在 K 上的次数为 d，模 $\mathfrak{p}$ 的约化为$x \mapsto (x^{p^2} + \bar{s})/\bar{c}$。

令 h 为 $\mathbb{P}^1(K)$上的绝对对数魏尔高度，并且

$$\widehat{h}_\varphi(\beta) = \lim_{n\to\infty} d^{-n} h\big(\varphi^n(\beta)\big)$$

$\widehat{h}_\varphi$ 点的典范高度 φ [4]。它满足 $h_\varphi \circ \varphi = d\, h_\varphi$，在 $\mathrm{Gal}(K/K)$ 作用下保持不变，因为 φ 定义在 K上，并且 $h_\varphi(\beta) = 0$ 恰当当且仅当 β 是前周期的，这由诺斯科特定理得出。对于 $\alpha \in \mathbb{P}^1(\overline{K})$，我们记作

$$\alpha_n = \varphi^n(\alpha), \qquad D_n = [K(\alpha_n) : K], \qquad r_n = D_n / D_{n+1}.$$

由于 $K(\alpha_{n+1}) \subseteq K(\alpha_n)$，每个 r_n 都是整数；又因为 α_n 属于 $\varphi^{-1}(\alpha_{n+1})$，而该集合至多包含 d 个在 $\mathrm{Gal}(K/K(\alpha_{n+1}))$ 作用下稳定的点，所以 $r_n \le d$。

以下窗口界在§6中得到证明；只要轨道上连续 $h_\varphi(\alpha)$ 步的次数保持不变，它就从下方界定 $\asymp \sqrt{\log D}$。

定理 2.1。存在常数 c_1'、$c_2 > 0$ 以及非递减函数 $k(D) = k_0 + \lceil B\sqrt{\log 3D}\,\rceil$，其中 k_0、B 仅取决于 Φ、K 和 $\mathfrak{p}$，使得以下结论成立。设$\alpha \in \mathbb{P}^1(K)$ 对于 φ不是前周期的，并设 $m \ge 0$ 满足：对于 $0 \le i \le k(D_m)$，有 $D_{m+i} = D_m$。则

$$\widehat{h}_\varphi(\alpha) \;\ge\; \mathcal{B}(D_0) \prod_{n<m} \frac{r_n}{d}, \qquad \mathcal{B}(D) = \frac{c_1'}{D} \exp\!\big(-c_2\sqrt{\log 3D}\big).$$

特别地，如果 $D_n = D_0$ 对于 $0 \le n \le k(D_0)$，那么 $h_\varphi(\alpha) \ge \mathcal{B}(D_0)$；而且，使用 $r_n = d$ 的步骤不会降低下界。

常数在§6中明确给出。证明占据§§3–6：我们构造轨道的特征形式 A_n，其零点是 K的共轭元；证明同余 α_n，并将其与阿基米德估计进行比较。

3. Binary forms and push-forward

本节回顾二元形式和结式，并定义由一对形式对一个形式所作的推前；该推前的零点是该形式的零点的像。

设 R 为交换环。R 上的一个次数为 D 的二元形式是 $A = \sum_{i=0}^{D} a_i X^i Z^{D-i} \in R[X, Z]$。对于 R 的理想 I，当 $A - B$ 的所有系数都属于 I时，我们写作 $A \equiv B \pmod{I}$。如果 $R = \mathcal{O}$ 是离散赋值环，那么当某个系数为单位元时，A 是本原的；根据高斯引理，本原形式的乘积仍是本原的。

对于次数为 A 的形式和次数为 G 的形式，$\mathrm{Res}(A, G)$ 表示西尔维斯特结式。它是关于 A 和 G 的系数、系数为整数的多项式；关于 A 的系数是次数为 δ 的齐次多项式，关于 G 的系数是次数为 D 的齐次多项式，并且对每个自变量都具有乘法性。在一个域上，如果 $A = \prod_{i=1}^{D}(z_i X - x_i Z)$，那么

$$\mathrm{Res}(A, G) = \pm \prod_{i=1}^{D} G(x_i, z_i), \tag{2}$$

符号仅取决于 D 和 δ。代数闭域上的每个非零形式都可以按这种方式分解。

形式 A 通过一对 Φ的推前是一个形式，其零点是 Φ下 A的零点的像。

定义 3.1。设 $\Phi = (\Phi_0,\ \Phi_1)$ 是域 R 上次数为 δ 的一对二元形式。对于域 R 上次数为 D 的形式 A，令

$$\Phi_* A(X,Z) \ = \ \mathrm{Res}_{(x,z)}\big(A(x,z),\ X\,\Phi_1(x,z) - Z\,\Phi_0(x,z)\big),$$

结式取关于变量 $(x,\ z)$ 计算，系数属于 $R[X,Z]$。

由于第二个自变量关于 $(X,\ Z)$ 是线性的，$\Phi_* A$ 是次数为 D的形式。其系数是以 A 和 Φ 的系数以及 $\Phi_*(\lambda A) = \lambda^\delta \Phi_* A$的系数为变量、具有整数系数的多项式。在一个域上，(2) 给出

$$\Phi_* \prod_{i=1}^{D} (z_i X - x_i Z) \ = \ \pm \prod_{i=1}^{D} \big(\Phi_1(x_i,z_i)X - \Phi_0(x_i,z_i)Z\big). \tag{3}$$

因此，如果 $\Phi_0,\ \Phi_1$ 在 $\mathbb{P}^1$ 中没有公共零点，那么 $\Phi_* A$ 恰好在 Φ 下 A 的零点的像处消失，并且重数相同。

下一个引 理将两个形式之间的同余转化为其结果式的整除性 t.

引理 3.2。设 $\mathcal{O}$ 是一个离散赋值环，I 是 $\mathcal{O}$ 的一个理想。设 A、$B \in \mathcal{O}[X,Z]$ 的次数为 D，其中 $A \neq 0$；并设 $B \equiv \mu A$（模 I^m），其中 $\mu \in \mathcal{O}$。则 $\mathrm{Res}(A,\ B) \ \in I^{mD}$。

证明。将 $B = \mu A + C$ 写成其系数在 I^m 中的 C。在分式域的代数闭包上，写成 $A = \prod_i (z_i X - x_i Z)$。由（2），由于 $A(x_i, z_i) = 0$，$\mathrm{Res}(A,B) = \pm \prod_i B(x_i,z_i) = \pm \prod_i C(x_i,z_i) = \mathrm{Res}(A,C)$，符号相同，因为次数相同。由于 $\mathrm{Res}(A,C)$ 关于 C 的系数是次数为 D 的齐次形式，且其系数属于 $\mathcal{O}$，因此它属于 I^{mD}。□

4. Congruences for push-forwards

在本节中，我们将证明，由一对弗罗贝尼乌斯提升形式所诱导的推前，会使形式之间的同余提高 $\mathfrak{p}$的一次幂。

在本节中，R 是一个交换环，$I \subseteq R$ 是一个理想，且满足 $p \in I$；对于 $m \geq 0$，当 $A - B$ 的所有系数都属于 I^m 时（其中 $I^0 = R$），我们记作 $A \equiv B$ (模 I^m)。设 ζ 是一个本原的 p次单位根。我们利用$(1-\zeta)\mathbb{Z}[\zeta] \cap \mathbb{Z} = p\mathbb{Z}$。由于 $\mathbb{Z}[\zeta]$ 是一个自由的 $\mathbb{Z}$-模，对多项式逐系数也成立：若 $T \in \mathbb{Z}[\mathbf{a}][X,Z]$（其中变量集合任意，$\mathbf{a}$）属于$(1-\zeta)\mathbb{Z}[\zeta][\mathbf{a}][X,Z]$，则 $T \in p\mathbb{Z}[\mathbf{a}][X,Z]$。

令$\mathbf{a} = (a_0、\ldots\ldots、a_D)$为变量，$A = \sum a_i X^i Z^{D-i}$ 为一般形式。乘积$\prod_{j=0}^{p-1} A(\zeta^j X、Z)$在 $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ 作用下是不变量，该作用会置换各因子，因此其系数属于 $\mathbb{Z}[\mathbf{a}]$。它在 $X \mapsto \zeta X$ 作用下同样是不变量，因此只出现含有 $p \mid i$ 的单项式 $X^i Z^{pD-i}$ 。

因此，存在唯一一个在 $\mathbb{Z}[\mathbf{a}]$ 上次数为 D 的形式 $A^{[p]}$，满足

$$A^{[p]}(X^p, Z^p) = \prod_{j=0}^{p-1} A(\zeta^j X, Z).$$

对于任意环上的形式，我们通过专门化系数来定义 $A^{[p]}$。在域上，由$\prod_j(\zeta^j a - b) = (-1)^{p+1}(a^p - b^p)$,

$$\Big(\prod_{i=1}^{D}(z_i X - x_i Z)\Big)^{[p]} = \big((-1)^{p+1}\big)^D \prod_{i=1}^{D}\big(z_i^p X - x_i^p Z\big). \tag{4}$$

我们也记作 $A^{(p)} = \sum a_i^p X^i Z^{D-i}$。

形式 $A^{[p]}$ 的零点是形式 A的零点的 p次幂。下一个引理表明，它模 p同余于 $A^{(p)}$，并且它将关于 I的同余提高一阶。

引理 4.1。设 A、B 是域 R上的次数为 D 的形式。

(a) $A^{[p]} \equiv A^{(p)}$（模 pR）。(b) 若 $m \geq 1$ 且 $A \equiv B$（模 I^m），则 $A^{[p]} \equiv B^{[p]}$（模 I^{m+1}）。

证明。(a) 只需处理一般系数。模 $1-\zeta$，每个因子 $A(\zeta^j X,\ Z)$ 都与 $A(X,\ Z)$ 同余，并且 $A(X,\ Z)^p \equiv A^{(p)}(X^p,\ Z^p)$ 模 p 同余。因此 $A^{[p]}(X^p,\ Z^p) - A^{(p)}(X^p,\ Z^p)$ 的系数属于 $\mathbb{Z}[\mathbf{a}],$，故其属于 $(1-\zeta)\mathbb{Z}[\zeta][\mathbf{a}][X,Z]$，从而属于 $p\mathbb{Z}[\mathbf{a}][X,Z]$。

(b) 设 $H = \sum y_i X^i Z^{D-i}$ 为另一个一般形式，并分解为

$$\prod_{j=0}^{p-1}(A+H)(\zeta^j X, Z) = \Pi_0 + \Pi_1 + \Pi_{\geq 2},$$

其中 Π_1 收集 $\mathbf{y}$ 中次数为 $\mathbf{1}$ 的项，而 $\Pi_{\geq 2}$ 收集次数为 ≥ 2 的项。伽罗瓦共轭保持 $\mathbf{y}$ 的次数不变，因此每一部分的系数都属于 $\mathbb{Z}[\mathbf{a}, \mathbf{y}]$。此外，$\Pi_1 = \sum_j H(\zeta^j X, Z)\prod_{l\neq j} A(\zeta^l X, Z) \equiv pHA^{p-1} \equiv 0$ 模 $1-\zeta$，所以 $\Pi_1 \in p\mathbb{Z}[\mathbf{a}, \mathbf{y}][X,Z]$。现在作特化，使得 $A + H = B$；H 的系数属于 I^m。于是 Π_1 关于它们是线性的，且系数属于 $pR \subseteq I$，因此其系数属于 I^{m+1}；而 $\Pi_{\geq 2}$ 的每个系数都属于 $I^{2m} \subseteq I^{m+1}$，如 $m \geq 1$ 所示。因此，$B^{[p]}(X^p, Z^p) - A^{[p]}(X^p, Z^p) = \Pi_1 + \Pi_{\geq 2}$ 的系数属于 I^{m+1}。□

接下来，我们比较两对模 I 同余的形式所对应的推前。

引理 4.2. 设 Φ, Ψ 是次数为 δ 的形式对，定义在 R 上，且满足 $\Phi \equiv \Psi$（模 I）；A, B是次数为 D 的形式，且满足 $A \equiv B$（模 I^m），$m \geq 0$。那么 $\Phi_* A - \Psi_* A$ 的系数属于 I，并且

$$(\Phi_* A - \Psi_* A) - (\Phi_* B - \Psi_* B) \ \textit{has coefficients in } I^{m+1}.$$

证明。将 $\Phi = \Psi + H$写成关于 H 的 I，其**系数为 $\mathbf{h}$**。$\Phi_* A$ 的系数是整系数多项式 $\mathcal{R}(\mathbf{a}\ \boldsymbol{\psi} + \mathbf{h})$，根据泰勒展开，$\mathcal{R}(\mathbf{a}\ \boldsymbol{\psi} + \mathbf{h}) - \mathcal{R}(\mathbf{a}\ \boldsymbol{\psi}) = \sum_{\beta\neq 0} \mathbf{h}^\beta \mathcal{S}_\beta(\mathbf{a}\ \boldsymbol{\psi})$

其中 $\mathcal{S}_\beta$为整系数多项式。每个$\mathbf{h}^\beta$都属于 I，由此得到第一个断言。由于$\mathbf{b}-\mathbf{a}$在 I^m 中有元素， $\mathcal{S}_\beta(\mathbf{b}\ \psi)-\mathcal{S}_\beta(\mathbf{a}\ \psi)\in I^m$，由此得到第二个断言。□

结合前面的两个引理，我们证明了通过 Φ 推前会使同余的模数提高 $\mathfrak{p}$ 的一幂。

引理 4.3（提升引理）。设 Φ、Ψ、c、s 如（1）所示，并设 A、$B\in\mathcal{O}[X,Z]$ 的次数为D。

（a） $\Phi_*A\equiv\pm A^{(p^2)}$ $(cX-sZ,\ Z)$（模 $\mathfrak{p}$），其中 $A^{(p^2)}=(A^{(p)})^{(p)}$，且符号仅取决于 p 和 D。（b）若 $m\geq 1$、$\mu\in\mathcal{O}^\times$ 和 $A\equiv\mu B$（模 $\mathfrak{p}^m$），则 $\Phi_*A\equiv\mu^d\,\Phi_*B$（模 $\mathfrak{p}^{m+1}$）。

证明。首先我们证明恒等式

$$\Psi_*A=\varepsilon\,(A^{[p]})^{[p]}(cX-sZ,\,Z),\qquad \varepsilon=\pm1\text{ depending only on }p,D, \tag{5}$$

对于 A 上的每个形式和每个环均成立。两边都是（$\mathbf{a}$ c、s）中的整系数多项式，因此只需对复数值进行验证。记 $A=\prod_i(z_iX-x_iZ)$。由（3），

$$\Psi_*A=\pm\prod_i\big(cz_i^dX-(x_i^d+sz_i^d)Z\big)=\pm\prod_i\big(z_i^d(cX-sZ)-x_i^dZ\big),$$

并且将 (4) 应用两次，得到 $(A^{[p]})^{[p]}=\pm\prod_i(z_i^dX-x_i^dZ)$。这就证明了 (5)。

我们将前面的引理应用于 $R=\mathcal{O}$ 和 $I=\mathfrak{p}$，其中包含 p。

(a) 由引理 4.2，$\Phi_*A\equiv\Psi_*A$（模 $\mathfrak{p}$）。由引理 4.1(a)，$(A^{[p]})^{[p]}\equiv(A^{[p]})^{(p)}$（模 p），且由于 $a\equiv b$（模 p）蕴含 $a^p\equiv b^p$（模 p），再次由引理 4.1(a) 得到 $(A^{[p]})^{(p)}\equiv(A^{(p)})^{(p)}=A^{(p^2)}$（模 p）。由于 $p\in\mathfrak{p}$，代入 (5) 得到 (a)。

(b) 令 $A'=\mu B$，于是 $\Phi_*A'=\mu^d\Phi_*B$ 和 $A\equiv A'$（模 $\mathfrak{p}^m$）。写作

$$\Phi_*A-\Phi_*A'=(\Psi_*A-\Psi_*A')+\big[(\Phi_*A-\Psi_*A)-(\Phi_*A'-\Psi_*A')\big].$$

括号内的表达式的系数属于 $\mathfrak{p}^{m+1}$ 由引理4.2可知。由引理4.1(b) 连续应用两次，$(A^{[p]})^{[p]}\equiv(A'^{[p]})^{[p]}$(模 $\mathfrak{p}^{m+2}$)，且代换 $(X,Z)\mapsto(cX-sZ,Z)$ 的系数属于 $\mathcal{O}$，因此由 (5) 可知，第一项的系数属于 $\mathfrak{p}^{m+2}$。□

5. The growing congruence

本节证明，在 φ 的轨道上，特征形式满足一个同余关系，其模数在每一步都增加 $\mathfrak{p}$ 的一个幂次。

5.1. 周期。令 σ_p 为 k 上的映射 $y\mapsto y^p$，并令 $\bar c,\bar s\in k$ 为 c,s 的约化。定义 Θ: $k^\times\times k\to k^\times\times k$ 为

$$\Theta(x,y)=\big(\sigma_p^2(x)\,\bar c,\ \sigma_p^2(x)\,\bar s+\sigma_p^2(y)\big).$$

对于一个形式 B在 k上置换 $T(B)(X,\ Z)=B^{\sigma_p^2}(\bar cX-\bar sZ,\ Z)$，其中 $B^{\sigma_p^2}$作用于 σ_p^2系数。根据引理 4.3(a)，T 描述了 Φ_* 在约化上的作用。

T的某个幂，因此 Φ_*的约化的某个幂，是恒等变换。

引理 5.1. 存在最小整数 $q \geq 1$，使得 $\Theta^q(1,0) = (1,0)$ 且 $f \mid 2q$。它只取决于 $\bar{c}$、$\bar{s}$ 和 k，并且对于 k 上的任意形式 B，都有 $T^q(B) = B$。

证明。有限集 $k^\times \times k \times \mathbb{Z}/f\mathbb{Z}$ 上的映射 $(x, y, j) \mapsto (\Theta(x, y)\ j + 2)$ 是双射；其逆元是显式的。因此，$(1, 0, 0)$ 的轨道是纯周期的，其周期是陈述中所述的最小 q。由归纳法，$T^n(B) = B^{\sigma_p^{2n}}(\gamma_n X - \delta_n Z,\ Z)$，其中 $(\gamma_n, \delta_n) = \Theta^n(1, 0)$：事实上

$$T\big(B^{\sigma_p^{2n}}(\gamma_n X - \delta_n Z, Z)\big) = B^{\sigma_p^{2n+2}}\big(\sigma_p^2(\gamma_n)(\bar{c}X - \bar{s}Z) - \sigma_p^2(\delta_n)Z,\ Z\big).$$

对于 $n = q$，这是 $B^{\sigma_p^{2q}}$，它等于 B，因为 σ_p^f 在 k 和 $f \mid 2q$ 上是恒等映射。 □

5.2. **同余。** 对于形式 A 在 $\mathcal{O}$ 上，我们记 $\Phi_*^n A$ 为 n重推前（定义 3.1）。

现在我们沿着轨道证明增长的同余。

定理 5.2（增长同余）。设 $A \in \mathcal{O}[X, Z]$ 是一个本原形式，并令 $A_n = \Phi_*^n A$。则：

（i）每个 A_n 都是本原的；（ii）对于每个 $n \geq 0$，存在 $\mu_n \in \{\pm 1\}$ 使得 $A_{n+q} \equiv \mu_n A_n$（模 $\mathfrak{p}^{n+1}$）。

证明。用横线表示模 $\mathfrak{p}$约化。引理 4.3（a）给出 $\Phi_* B = \pm T(B)$，对每个在 $\overline{\mathcal{O}}$ 上的形式 B 都成立。映射 T 是单射，因为σ_p 是单射且代换可逆，并且 $T(-B) = -T(B)$。

(i) 根据归纳法，$\overline{A_{n+1}} = \pm T(\overline{A_n}) \neq 0$。

(ii) 对于 $n = 0$，引理 5.1 给出$\overline{A_q} = \pm T^{\overline{q}}(A) = \overline{\pm} A$。假设 $A_{n+q} \equiv \mu_n A_n$ (模 $\mathfrak{p}^{n+1}$)。引理 4.3(b)，结合 $m = n + 1$，给出 $A_{n+1+q} \equiv \mu_n^d A_{n+1}$ (模 $\mathfrak{p}^{n+2}$)，以及 $\mu_n^d = \pm 1$。 □

5.3. **极小形式与结式。** 对于 $\beta \in \mathbb{P}^1(K)$，设 $F_\beta \in \mathcal{O}[X, Z]$ 为一个本原形式，它在 K 上不可约，并在 β 处取零点；除相差一个 $\mathcal{O}^\times$ 外它是唯一的。其次数为 $[K(\beta) : K]$，其零点是 β 的 K-共轭元，且每个都是单零点。

递增同余给出了轨道中两个点的极小形式的结式的 $\mathfrak{p}$-进赋值的一个下界。

命题 5.3。 令 $\alpha \in \mathbb{P}^1(K)$ 对于 $\overline{\varphi}$ 不是前周期的，且 $F_n = F_{\alpha_n}$。令 $0 \leq n < m$ 满足 $m \equiv n$（模 q）。则 $\mathrm{Res}(F_m, F_n) \neq 0$，并且

$$v_\mathfrak{p}\big(\mathrm{Res}(F_m, F_n)\big) \geq (n+1)\,\frac{D_n D_m}{D_0},$$

其中，$v_\mathfrak{p}$ 通过 $v_\mathfrak{p}(\mathfrak{p}) = 1$ 进行归一化。

证明。设 $A = F_0$ 且 $A_n = \Phi_*^n A$。我们首先证明 $A_n = \kappa_n F_n^{D_0/D_n}$ 且 $\kappa_n \in \mathcal{O}^\times$。由（3），由于 Φ_0，Φ_1 没有公共零点，A_n 的零点是这些点：$\varphi^n(\gamma)$，其中 γ 遍历

的零点 A，也就是说，遍历 K共轭元 $\alpha_\circ$ 由于 $K(\alpha_n) \subseteq K(\alpha)$，每个 K共轭元 α_n出现 D_0/D_n 次。因此 A_n 和 $F_n^{D_0/D_n}$是定义在 K 上的次数相同且零点相同的形式，并且 $A_n = \kappa_n F_n^{D_0/D_n}$且 $\kappa_n \in K^\times$。根据定理 5.2（i）和高斯引理，两者都是本原的，因此 $\kappa_n \in \mathcal{O}^\times$。

令 $m = n + jq$。在 $n, n+q, \ldots, n+(j-1)q$ 处应用定理 5.2(ii)，并利用 $\mathfrak{p}^{n+iq+1} \subseteq \mathfrak{p}^{n+1}$，得到 $A_m \equiv \pm A_n$(模 $\mathfrak{p}^{n+1}$)。由引理 3.2，$v_\mathfrak{p}(\mathrm{Res}(A_n, A_m)) \geq (n+1)D_0$。由乘法性，$\mathrm{Res}(A_n, A_m)$ 等于一个单位元乘以 $\mathrm{Res}(F_n, F_m)^{(D_0/D_n)(D_0/D_m)}$，从而得到该不等式。

如果 $\mathrm{Res}(F_m, F_n) = 0$，那么对某个 $\overline{\gamma} \in \mathrm{Gal}(K/K)$，有 $\alpha_m = \gamma(\alpha_n)$。由于 $h_\varphi \circ \varphi = d\, h_\varphi$ 和 $h_{\overline{\varphi}}$ 在 $\mathrm{Gal}(K/K)$ 下是不变量，因此得到 $d^m h_\varphi(\alpha) = d^n h_\varphi(\alpha)$，所以 $h_\varphi(\alpha) = 0$，且 α 是前周期的，矛盾。□

6. Green functions and the proof of Theorem 2.1

在本节中，我们将§5 的同余与长度为 $\asymp \sqrt{\log D}$ 步的窗口上的阿基米德能量估计进行比较。

6.1. 绝对值和格林函数。 对于每个赋值 $\ell \leq \infty$，$\mathbb{Q}$令 $\mathbb{C}_\ell$ 为 $\mathbb{C}$（若$\ell = \infty$），否则为 $\mathbb{Q}_\ell$ 的代数闭包的完备化。对于数域 L'，每个嵌入 $\sigma\colon L' \hookrightarrow \mathbb{C}_\ell$ 给出一个绝对值 $|x|_\sigma = |\sigma x|_\ell$，其中 $|\ell|_\ell = \ell^{-1}$ 且$|\cdot|_\infty$ 是通常的绝对值；而 L' 上方的 ℓ 的赋值 w 恰好来自 $[L'_w$ 个 $\mathbb{Q}_\ell]$: 嵌入。我们记 $\sum_\sigma$ 为将 L' 嵌入所有 $\mathbb{C}_\ell$中的所有嵌入之和。乘积公式为：对于 $x \in L'^\times$，$\sum_\sigma \log|x|_\sigma = 0$；而 $\beta \in \mathbb{P}^1(L')$ 的高度（带有提升$\tilde{v} \in L'^2$）为 $h(\beta) = [L' : \mathbb{Q}]^{-1} \sum_\sigma \log \|\sigma\tilde{v}\|$，其中 $\|\cdot\|$ 为最大范数。

对于嵌入 $\iota\colon K \hookrightarrow \mathbb{C}_\ell$令 Φ^ι 为将系数作用以 ι 后得到的一对；对于 $v \in \mathbb{C}_\ell^2 \setminus \{0\}$，令 $\widehat{H}_\iota(v) = \lim_n d^{-n} \log \|(\Phi^\iota)^{(n)}(v)\|$，并令 $r_\iota = d^{\frac{1}{(d-1)}} \log |\iota \mathrm{Res}(\Phi)|_\infty$ 仿照 Baker [1, (1.6)],，对于带有提升 $\tilde{z}, \tilde{z}'$ 的互异 $z, z' \in \mathbb{P}^1(\mathbb{C}_\ell)$，令

$$g_\iota(z, z') = -\log|\tilde{z} \wedge \tilde{z}'| + \widehat{H}_\iota(\tilde{z}) + \widehat{H}_\iota(\tilde{z}') - r_\iota,$$

其中 $(v_0, v_1) \wedge (v'_0, v'_1) = v_0 v'_1 - v_1 v'_0$；由下文的 (G1) 可知，它不依赖于这些提升。令 $\mathcal{S}$为 K 的有限集赋值，这些赋值是阿基米德赋值，或使得 Φ 的某个系数不为整数，或整除 $\mathrm{Res}(\Phi)$。根据 §2，$\mathfrak{p} \notin \mathcal{S}$。我们使用以下事实。

(G1) $H_\iota(\Phi^\iota(v)) = d\, H_\iota(v)$ 以及 $H_\iota(\lambda v) =$ 对数 $|\lambda| + H_\iota(v)$。（G2）如果 ι 在 $\mathcal{S}$之外诱导出 K的一个赋值，那么 $\widehat{H}_\iota(v) =$对数 $\|v\|$，$r_\iota = 0$，并且 $g_\iota(z, z') = -$对数$\left(|\tilde{z} \wedge \tilde{z}'|/\|\tilde{z}\|\|\tilde{z}'\|\right) \geq 0$。（G3）对于数域 $L' \supseteq K$，$\beta \in \mathbb{P}^1(L')$ 以及一个提升 $\tilde{v} \in L'^2$，$\sum_\sigma \widehat{H}_{\sigma|_K}(\sigma\tilde{v}) = [L' : \mathbb{Q}]\, \widehat{h}_\varphi(\beta)$，其中 $\widehat{h}_\varphi(\beta) =$ 极限 $_n\, d^{-n} h(\varphi^n(\beta))$。（G4）（Baker [1, 定理 1.1]）对于每个 ι，存在 $C_\iota \geq 0$，当 ι 在 $\mathcal{S}$之外诱导出一个赋值时满足 $C_\iota = 0$，使得对于所有互不相同的 z_1，……，$z_M \in$，$\sum_{i \neq j} g_\iota(z_i, z_j) \geq -C_\iota M$对数 M，$\mathbb{P}^1(\mathbb{C}_\ell)$。

（G1）–（G3）是 Call–Silverman 典范高度及其局部分解的标准性质 [4]；在（G2）中，不等式是超度量不等式；在（G3）中，可以将极限与求和交换，这是因为根据（G2），只有有限多个赋值的贡献不是对数 $\|\sigma\tilde{v}\|$。Baker 定理 1.1 对于关于非平凡绝对值完备的任意代数闭域都成立，特别是在每个 $\mathbb{C}_\ell$上成立，其中常数取决于映射和域，并且其求和遍历有序对；对于 ι之外的 $\mathcal{S}$，由（G2）可得（G4）。我们将 $\sum_{i\neq j} g_\iota(z_i,\ z_j)$ 称为 能量，其对应于 z_1, ……, z_M在 ι处。令

$$C=\max\Big\{1,\ \frac{1}{[K:\mathbb{Q}]}\sum_{\iota}C_\iota\Big\},\qquad \lambda_{\mathfrak{p}}=\frac{\log N\mathfrak{p}}{[K:\mathbb{Q}]},$$

对 K 嵌入到所有 $\mathbb{C}_\ell$ 的嵌入求和；只有有限项非零。我们固定常数 C_ι，并在下文始终使用这些常数；下文所有常数均取决于这一选择。

6.2. 参数的选择。 令 $B=\sqrt{12qC/\lambda_{\mathfrak{p}}}$，使得 $\lambda_{\mathfrak{p}}B^2/(3q)=4C$，令 $k_1\geq 1$ 为满足 $\lambda_{\mathfrak{p}}k_1^2/(3q)\geq C\log(3q+k_1+2+B)$ 的最小整数，并定义

$$k(D)=3q+k_1+\big\lceil B\sqrt{\log 3D}\,\big\rceil,\qquad \mathcal{B}(D)=\frac{c_1'}{D}\exp\big(-c_2\sqrt{\log 3D}\big),$$

其中 $c_1'=\frac{3}{4}d^{-(3q+k_1+1)}$，且 $c_2=B\log d$。

下一个引理给出了决定窗口长度 $k(D)$ 选择的不等式。

引理 6.1。 对于每个整数 $D\geq 1$ 以及 $k=k(D)$，

$$\frac{\lambda_{\mathfrak{p}}}{3q}(k+2)(k-3q)-C\log\big((k+1)D\big)\ \geq\ 2C\log 3D.$$

证明。令 $u=k-3q\geq k_1+B\sqrt{\log 3D}$。于是 $(k+2)(k-3q)\geq u^2\geq k_1^2+B^2\log 3D$，因此第一项至少为 $\lambda_{\mathfrak{p}}k_1^2/(3q)+4C\log 3D$。接下来，$k+1\leq 3q+k_1+2+B\sqrt{\log 3D}\leq(3q+k_1+2+B)(1+\log 3D)$，且 $\log(1+x)\leq x$，所以 $\log((k+1)D)\leq\log D+\log(3q+k_1+2+B)+\log 3D\leq 2\log 3D+\log(3q+k_1+2+B)$。取 k_1 即得结论。□

6.3. 窗口界。 我们首先证明从第一步开始的窗口的窗口界。

命题 6.2. 设 $\alpha\in\mathbb{P}^1(K)$ 不是 φ的前周期点，并假设 $D_n=D_0$ *for* $0\leq n\leq k(D_0)$。则 $h_\varphi(\alpha)\geq\mathcal{B}(D_0)$。

证明。记 $D=D_0$ 和 $k=k(D)$。令 S_n 为 α_n的 D 个互异的 K-共轭元、$F_n=F_{\alpha_n}$的零点以及 $S=S_0\cup\cdots\cup S_k$所组成的集合。令 L' 为一个有限 Galois 扩张，其为 K 的扩张，且 S 的所有点都在其中定义；对每个 $\beta\in S$ 固定一个提升 $\tilde{v}_\beta\in L'^2$。对于 L' 的一个嵌入 σ，记 $g_\sigma(\beta,\beta')=g_{\sigma|_K}(\sigma\beta,\sigma\beta')$。

的一个共轭元 α_n 永远不是 α_m 的共轭元，其中 $n\neq m$ （命题5.3的证明结尾 S 有 $N=(k+1)D$ 个元素，并且 $N\geq 2$ 因为 $k\geq 1$。

我们断言

$$\sum_{\sigma}\sum_{\beta\neq\beta'\in S} g_\sigma(\beta,\beta') = 2(N-1)\,[L':\mathbb{Q}]\,D\sum_{n=0}^{k}\widehat{h}_\varphi(\alpha_n). \tag{6}$$

事实上，根据乘积公式，$-\log|\tilde{v}_\beta\wedge\tilde{v}_{\beta'}|_\sigma$ 在 σ 上求和为 0，因为 $\tilde{v}_\beta\wedge\tilde{v}_{\beta'}\in L'^{\times}$；根据 $\mathrm{Res}(\Phi)\in K^\times$，$r_{\sigma|_K}$也满足同样结论。每个 β 出现在 $2(N-1)$ 个有序对中，因此根据 (G3)，H 贡献 $2(N-1)[L':\mathbb{Q}]\sum_{\beta\in S}h_\varphi(\beta)$，并且对于 $\beta\in S_n$，$h_\varphi(\beta)=h_\varphi(\alpha_n)$。

每个嵌入 ι 的 K 延拓到 $[L':K]$ 个嵌入 σ 的 L'，且每个 $\sigma(S)$ 由N 个不同的点组成。由 (G2) 和 (G4)，其限制到 后在 $\mathcal{S}$中诱导出一个赋值的嵌入 $-[L'$至少贡献 $K]\sum_\iota C_\iota N\log N\geq -[L':\mathbb{Q}]\,C\,N\log N$到 (6) 的左侧，而对于所有其他嵌入，每一对贡献 ≥ 0。

设 σ 是从 L' 到 $\mathbb{C}_p$ 的一个嵌入，并在 K 上诱导出 $\mathfrak{p}$，再设 $0\leq n<m\leq k$ 满足 $m\equiv n$（模 q）。$\sigma(S_m)$ 和 $\sigma(S_n)$ 的点分别是 σF_m 和 σF_n 的零点；这两个形式的系数属于 $\mathbb{C}_p$ 的赋值环，且各自有一个单位元系数。由于 g_σ 与提升无关，我们可以使用由这些形式在 $\mathbb{C}_p$ 上分解为一次因子 z_iX-x_iZ 所得到的提升来计算它；根据高斯范数在 $\mathbb{C}_p[X,Z]$ 上具有乘法性，可以选取这些提升使得 $\|(x_i,z_i)\|=1$。于是，(G2) 和 (2) 表明，在两个顺序下，一个点处于层级 m、另一个点处于层级 n 的点对，其贡献为

$$-2\log\big|\mathrm{Res}(F_m,F_n)\big|_\sigma=\frac{2\log p}{e}\,v_{\mathfrak{p}}\big(\mathrm{Res}(F_m,F_n)\big)\;\geq\;\frac{2\log p}{e}\,(n+1)D$$

根据命题 5.3，有 $D_n=D_m=D$。所有其他点对的贡献为 ≥ 0。从 L' 到 $\mathbb{C}_p$、在 K 上诱导出 $\mathfrak{p}$ 的嵌入数量为 $[L':K]\,[K_{\mathfrak{p}}:\mathbb{Q}_p]=[L':K]\,ef$。因此，这些嵌入的贡献至少为

$$2[L':K]\,D\log N\mathfrak{p}\sum_{\substack{0\leq n<m\leq k\\ m\equiv n\ (q)}}(n+1)\;\geq\;2[L':K]\,D\log N\mathfrak{p}\cdot\frac{(k+1)(k+2)(k-3q)}{6q},$$

利用 $\sum_{n<m\leq k,\ q\mid m-n}(n+1)\geq\sum_{n=0}^{k}(n+1)\big(\frac{k-n}{q}-1\big)=\frac{(k+1)(k+2)(k-3q)}{6q}$。

(6) 的右侧，$\widehat{h}_\varphi(\alpha_n)=d^n\widehat{h}_\varphi(\alpha)$，因此 $\sum_{n\leq k}\widehat{h}_\varphi(\alpha_n)\leq\frac{4}{3}d^k\widehat{h}_\varphi(\alpha)$，因为 $d\geq 4$。合并后，除以 $[L':\mathbb{Q}](k+1)D$ 并利用 $N-1<(k+1)D$，

$$\tfrac{8}{3}\,D\,d^k\,\widehat{h}_\varphi(\alpha)\;\geq\;\frac{\lambda_{\mathfrak{p}}}{3q}(k+2)(k-3q)-C\log\big((k+1)D\big)\;\geq\;2C\log 3D\;\geq\;2$$

由引理 6.1，因为 $C\geq 1$ 且 $\log 3>1$。由于 $d^k\leq d^{3q+k_1+1}\exp(B\log d\sqrt{\log 3D})$，得到$\widehat{h}_\varphi(\alpha)\geq\mathcal{B}(D)$。□

定理 2.1 的证明。取 $k_0=3q+k_1$。命题 6.2 适用于 α_m，其轨道为 $(\alpha_{m+i})_{i\geq 0}$，并给出 $h_\varphi(\alpha_m)\geq\mathcal{B}(D_m)$。由于 $D_m\leq D_0$，$\mathcal{B}(D_m)\geq\mathcal{B}(D_0)D_0/D_m$。现在 $h_\varphi(\alpha_m)=d^m h_\varphi(\alpha)$ 且 $D_0/D_m=\prod_{n<m}r_n$。□

7. The Lattès map of multiplication by p

在本节中，我们证明由 $[p]$ 诱导的映射在 x线上满足假设（1），并且没有周期临界点。从现在起 E/K 与引言中的定义相同。

7.1. 除法多项式。 设 E 由 $y^2+a_1xy+a_3y=x^3+a_2x^2+a_4x+a_6$ 给出，其中$a_i\in\mathcal{O}$。我们按照 [16, Ex. 3.7] 使用除法多项式 ψ_n 和 $\phi_n=x\psi_n^2-\psi_{n+1}\psi_{n-1}$。我们需要以下事实。多项式 ψ_n^2和 ϕ_n属于 $\mathbb{Z}[a_1,\dots,a_6][x]$； ϕ_n是次数为 n^2 的首一多项式，而 ψ_n^2 的次数至多为 n^2-1，其 x^{n^2-1}-系数为 n^2 [16, Ex. 3.7]。按这些形式次数计算，它们的结式为

$$\operatorname{Res}(\phi_n,\psi_n^2)=\pm\Delta^{n^2(n^2-1)/6} \tag{7}$$

（见 [5] 和 [16, Ex. 3.7]）。恒等式 $x\circ[n]=\phi_n/\psi_n^2$ 在 $\mathbb{Z}[a_1,\dots,a_6,\Delta^{-1}]$上的泛椭圆曲线上成立。根据（7），将其专门化到任意含有$\Delta\neq 0$的域上的魏尔斯特拉斯方程后，多项式 ϕ_n 和 ψ_n^2 仍无公共零点，因此该恒等式也可专门化：在每个域上，对于每个魏尔斯特拉斯方程，ψ_n^2 不是零多项式，并且 $x\circ[n]=\phi_n/\psi_n^2$作为曲线上的有理函数成立。

回忆 $d=p^2$，并令

$$\Phi_0(X,Z)=Z^d\phi_p(X/Z),\qquad \Phi_1(X,Z)=Z^d\psi_p^2(X/Z).$$

这些是次数为 d的二元形式，且 Z 整除 Φ_1。

在特征 0 中，形式 Φ_0，Φ_1 定义了 $[p]$的 Latt`es 映射。

引理 7.1。 在特征为0 的域上，形式 Φ_0和Φ_1 在 $\mathbb{P}^1$中没有公共零点，并且对每个点 P都有 $x([p]P)=\Phi(x(P))$，其中 $x(O)=(1:0)$。

证明。 函数 $x\circ[p]$ 在 E上的次数为 $2p^2$，因为 $[p]$ 的次数为 p^2，而 x 的次数为 2。它等于 $g\circ x$，其中 $g=\phi_p/\psi_p^2$，因此 g的次数为 p^2。如果 ϕ_p和 ψ_p^2有一个次数为$m\geq 1$的公因子，那么约去该因子后，分子次数将为 p^2-m，分母次数至多为 p^2-1-m，所以 g的次数将为 $p^2-m<p^2$。因此 ϕ_p和 ψ_p^2互素，并且由于 $\Phi_0(1,0)=1$，这些形式没有公共零点。对于 $P\neq O$，其中 $\psi_p^2(x(P))\neq 0$， $x([p]P)$的公式成立；对于其他点，两边均为 $(1:0)$，这是利用 $\Phi(1,0)=(1,0)$以及对于 $P\in E[p]\setminus\{O\}$，由互素性可知 $\phi_p(x(P))\neq 0$ 得到的。□

在特征为 p 的超奇异曲线上，乘以 p 是纯不可分的，这迫使其在 x-线上诱导的映射具有以下形式。

引理 7.2。 设 k 是特征为 p 的域，且 E/k 是由一个魏尔斯特拉斯方程给出的超奇异椭圆曲线。则存在 $c\in k^\times$ 和 $s\in k$，使得

$$\phi_p=x^{p^2}+s,\qquad \psi_p^2=c\qquad in\ k[x].$$

等价地， $\Phi_0=X^d+sZ^d$和 $\Phi_1=cZ^d$，以及 $x\circ[p]=\left(x^{p^2}+s\right)/c$。

证明。由于 $\widetilde{E}$ 是超奇异的， $\widetilde{E}[p](\bar{k}) = 0$ [16, V.3.1]。同源 $[p]$ 的次数为 p^2 [16,III.6.2], ，其可分次数等于其核中的点的数目 [16, III.4.10], ，即为1。因此， $[p]$ 是次数为 p^2的纯不可分同源，并且根据 [16,II.2.12]，它可分解为 $[p] = \lambda \circ \pi$，其中π: $\widetilde{E} \to \widetilde{E}^{(p^2)}$是 p^2次弗罗贝尼乌斯，而 λ 是次数为1的同源，因而是椭圆曲线的同构。由魏尔斯特拉斯方程给出的曲线之间的同构具有$x = u^2x' + r$ 的形式，其中 $u \in \bar{k}^\times$、 $r \in \bar{k}$ [16, III.3.1]。由于$x' \circ \pi = x^{p^2}$，我们得到 $x \circ [p] = u^2x^{p^2} + r$ 在$\bar{k}(x)$中。另一方面， $x \circ [p] = \phi_p/\psi_p^2$，其中 $\psi_p^2 \neq 0$。因此 $\phi_p = (u^2x^{p^2} + r)\psi_p^2$。左边是首一的、次数为 p^2的多项式；如果 ψ_p^2 的次数为 $m \geq 1$，则右边的次数将为 $p^2 + m$。所以$\psi_p^2 = c \in k^\times$，比较系数得到 $cu^2 = 1$ 和$\phi_p = x^{p^2} + s$，其中 $s = cr \in k$。□

7.2. **勒`映射提升弗罗贝尼乌斯。** 的魏尔斯特拉斯方程 E 的系数属于 $\mathcal{O}$，因此 Φ 的所有系数都属于 $\mathcal{O}$，而 Φ 的约化是以相同方式附属于~ ~E的一对。选取提升 c， $s \in \mathcal{O}$，它们是引理 7.2 中给出的元素针对 E的提升。则 $c \in \mathcal{O}^\times$ 并且

$$\Phi \equiv \Psi = \left(X^d + sZ^d,\ cZ^d\right) \pmod{\mathfrak{p}}.$$

因此 Φ 满足（1），且§§2–6 中的所有结果都适用于映射 φ，它由 Φ定义，是勒`映射，其$[p]$。根据引理 7.1， $x([p]Q) = \varphi(x(Q))$ 对所有 $Q \in E(K)$ 都成立。对于 $P \in E(K)$，我们记为

$$\alpha_n = \varphi^n(x(P)) = x([p^n]P), \qquad D_n = [K(\alpha_n) : K], \qquad r_n = D_n/D_{n+1},$$

如 §2中所示。

勒`映射的典范高度是 N´eron–Tate 高度的两倍。

引理 7.3。 对于每个 $Q \in E(K)$， $h_\varphi(x(\{v16'>)) = 2h_E(Q)$。特别地， $x(Q)$ 对于 φ 是前周期的，当且仅当 Q 是挠点。

证明。 N´eron–Tate 高度满足 $\widehat{h}_E(Q) = \frac{1}{2}h(x(Q)) + O(1)$，且 $\widehat{h}_E([p]Q) = p^2\widehat{h}_E(Q)$ [16,VIII.9.3]。因此 $d^{-n}h(\varphi^n(x(Q))) = p^{-2n}h(x([p^n]Q)) = 2\widehat{h}_E(Q) + O(p^{-2n})$。最后一个断言成立，因为 h_E 恰好在扭点处为零。对 h_E 采用其他规范化方式只会改变我们结果中的常数，不会改变指数。□

最后，Latt`es 映射的临界点来自 2-扭点，而且没有一个是周期点。

引理 7.4。 *Latt`es* 映射 φ 没有周期的临界点。

证明。映射 x: $E \to \mathbb{P}^1$ 的次数为 2，且恰好在 $E[2]$处分歧，而 $[p]$ 是未分歧的，因为我们处于特征 0 中。对于 $Q \in E(K)$，记映射g 在 z处的分歧指数为 $\mathrm{ram}_g(z)$，恒等式 $\varphi \circ x = x \circ [p]$ 给出 $\mathrm{ram}_\varphi(x(Q))\,\mathrm{ram}_x(Q) = \mathrm{ram}_x([p]Q)$。因此，当且仅当 $[p]Q \in E[2]$ 和 $Q \notin E[2]$时， $x(Q)$才是 φ 的临界点。于是，对于$n \geq 1$，有 $\varphi^n(x(Q)) = x([p^n]Q) \in x(E[2])$，并且 $x(E[2])$在 φ下是稳定的；但 $x(Q) \notin x(E[2])$，因为 $x(Q) = x(T)$迫使 $Q = \pm T$成立。因此， $x(Q)$不是周期的。最后， φ 在 $\mathbb{P}^1(\mathbb{C}_p)$中的每个临界点都是 K上的非零形式 $\partial_X\Phi_0\,\partial_Z\Phi_1 - \partial_Z\Phi_0\,\partial_X\Phi_1$的零点，因此位于 $\mathbb{P}^1(K)$中。□

8. Local dynamics at $\mathfrak{p}$

本节中 Φ、 c、 s 和 φ均如（1）中所述，例如 Latt`es 对以及§7中的映射，以及$d = p^2$。我们描述 φ 在 $\mathbb{P}^1$（$\mathbb{C}_p$）的剩余圆盘上的动力学：的约化置换这些剩余类，每个剩余圆盘恰好包含一个周期点，并且轨道以取决于分歧的速率趋近这些周期点。

令 $\mathbb{C}_p$ 为 $K_{\mathfrak{p}}$的代数闭包的完备化，固定一个在 K上的嵌入 $K \hookrightarrow \mathbb{C}_p$ ，令 v 为满足 $v(p) = 1$的赋值，并令 $\mathcal{O}_{\mathbb{C}_p}$ 为赋值环。对于 $\mathbb{C}_p$ 上的形式或矩阵 H，令 $v(H)$为其系数的最小赋值。由于对于 $\mathcal{O}$的一致化子 π有 $v(\pi) = 1/e$ ，假设 (1) 表明 $v(\Phi - \Psi) \geq 1/e$，其中

$$\Psi = \left(X^d + sZ^d,\ cZ^d\right) = G_0 \circ (X^d, Z^d), \qquad G_0 = \begin{pmatrix} 1 & s \\ 0 & c \end{pmatrix} \in \mathrm{GL}_2(\mathcal{O}).$$

Put

$$\rho(u) = \min\{du,\ u + 1/e\} \qquad (u \geq 0),$$

一个递增函数，且对于 $u > 0$，有 $\rho(u) > u$ 。

每个 $P \in \mathbb{P}^1(\mathbb{C}_p)$ 都有一个本原代表元（x_0， z_0），满足 $\min\{v(x_0)\ v(z_0)\} = 0$，其在单位元意义下唯一，并有一个约化 $\bar{P} \in \mathbb{P}^1(\mathbb{F}_p)$。对于 P， Q 及其本原代表元（x_0， z_0），（y_0， u_0），置

$$w(P, Q) = v(x_0u_0 - z_0y_0) \in [0, \infty].$$

那么， p^{-w}是弦度量，它是超度量；因此 $w(P,\ R) \geq \min\{w(P,\ Q)\ w(Q,\ R)\}$。此外， $w(P,\ Q) > 0$ 当且仅当 $\bar{P} = \bar{Q}$, w 在 $\mathrm{GL}_2(\mathcal{O}_{\mathbb{C}_p})$ 下是不变量，且 $\mathbb{P}^1(\mathbb{C}_p)$ 是完备的。对于 $\xi \in \mathbb{P}^1(\mathbb{F}_p)$，令 $U_\xi = \{P\colon\ \bar{P} = \xi\}$ 为其剩余圆盘。

第一个引理用局部坐标描述点附近的 φ ，并引入不变量 ϑ，它衡量 φ 在一点处分歧的程度。

引理 8.1。 (a)约化 $\bar{\varphi}$ 是 $\mathbb{P}^1(\mathbb{F}_p)$的双射，且 $\mathbb{P}^1(\mathbb{F}_p)$ 的每个点对它而言都是周期的；令 $\overline{q}_\xi$ 为 ξ的精确周期。

(b) 对于 $P \in \mathbb{P}^1(\mathbb{C}_p)$，取 $M_1, M_2 \in GL_2(\mathcal{O}_{\mathbb{C}_p})$，使得 $M_1(0) = P$且 $M_2(0) = \varphi(P)$，其中 $0 = [0\colon\ 1],$，并令 $(U_0, U_1) = M_2^{-1} \circ \Phi \circ M_1$, $a(t) = U_0(t, 1)$， $b(t) = U_1(t, 1)$。于是$a(0) = 0$, $b(t)$ 是 $v(t) > 0$的单位元，并且

$$a(t) = u\,t^d + t\,a_1(t), \qquad u \in \mathcal{O}_{\mathbb{C}_p}^\times, \quad a_1 \in \mathcal{O}_{\mathbb{C}_p}[t], \quad v(a_1) \geq 1/e.$$

(c) 对于 P、Q 且满足 $P = Q$: $w(\varphi P、\ \varphi Q) \geq \rho(w(P、\ Q))$。

(d) 在 *(b)* 的记号下， $\vartheta(P) = v(a'(0))$ 不依赖于 M_1、M_2 的选择，并且对于 P 的任一本原代表 $(x_0、\ z_0)$，$\vartheta(P) = v(J(x_0、\ z_0)) - 2$，其中 $J = \partial_X\Phi_0\,\partial_Z\Phi_1 - \partial_Z\Phi_0\,\partial_X\Phi_1$。有 $\vartheta(P) \geq 1/e$、$\vartheta(P) = \infty$ 当且仅当 P 是 φ 的临界点，并且存在 ϑ_0 ，使得对于有限多个剩余圆盘之外的所有 P， $\vartheta(P) = \vartheta_0$ 。

证明。 (a) 该约化为 $\bar{G}_0 \circ \mathrm{Frob}_p^2$，是 $\mathbb{P}^1(\mathbb{F}_p)$ 上双射的复合；这些双射对每个包含 $\mathbb{F}$ 的有限域都保持 $\mathbb{P}^1(\mathbb{F})$；在有限集 $\mathbb{P}^1(\mathbb{F})$ 上，双射即为置换。

(b) 对于 $M_1 = \left(\begin{smallmatrix} m_{00} & m_{01} \\ m_{10} & m_{11} \end{smallmatrix}\right)$，有 $(m_{00}X + m_{01}Z)^d \equiv m_{00}^d X^d + m_{01}^d Z^d$ 模 $p\,\mathcal{O}_{\mathbb{C}_p}[X,Z]$，因为 $p \mid \binom{d}{i}$ 当 $0 < i < d$ 时成立。因此，$\Psi \circ M_1 \equiv G_0 M_1^{(d)}(X^d,\ Z^d)$ 模 p，其中 $M_{(d)1}$ 的各项为 m_{ij}^d；又因为 $v(\Phi - \Psi) \geq 1/e$ 且 $1/e \leq 1$，

$$(U_0, U_1) \equiv \mu'\,(X^d, Z^d) \pmod{\{v \geq 1/e\}}, \qquad \mu' = M_2^{-1} G_0 M_1^{(d)},$$

且行列式 μ' 是单位元。由于 $\mathrm{Res}(\Phi_0, \Phi_1)$ 是单位元，$(U_0(P)\ U_1(P))$ 对每个本原的 $\tilde{P}$ 都是本原的；由于 $M_2^{-1}\varphi M_1$ 固定 0，$a(0) = 0$，且 $b(0)$ 是单位元。现在 $a(0) \equiv \mu'_{01}$，因此 $v(\mu'_{01}) \geq 1/e$ 且 μ'_{00}, μ'_{11} 都是单位元。对于 $v(t) > 0$，$b(t) \equiv \mu'_{10} t^d + \mu'_{11}$ 模极大理想是单位元。最后，$a(t) - \mu'_{00} t^d$ 的所有系数的赋值均为 $\geq 1/e$，且在 $t = 0$ 处消失；因此它等于 $t\,a_1(t)$，如所声称的，其中 $u = \mu'_{00}$。

(c) 在 (b) 中，$Q = M_1([t:1])$，其中 $v(t) = w(P,Q) > 0$，因为 w 是 $\mathrm{GL}_2(\mathcal{O}_{\mathbb{C}_p})$-不变量，且 $M_1^{-1}Q$ 位于 0 的剩余圆盘内。于是 $\varphi(Q) = M_2([a(t):b(t)])$，其中 $b(t)$ 是单位元，因此 $w(\varphi P, \varphi Q) = w([0:1],[a(t):b(t)]) = v\min\{dv(t)\ v(t) + 1/e\}$。

(d) 将 M_1 替换为固定 0 的 $M_1 \circ T$ $T \in \mathrm{GL}_2(\mathcal{O}_{\mathbb{C}_p})$，会使 $a'(0)/b(0)$ 乘以 $T'(0)$，其中后者是一个单位元；对 M_2 也同样如此；而 $b(0)$ 是一个单位元。由链式法则，$J_{M_2^{-1}\Phi M_1} = \det(M_2)^{-1}\det(M_1)\ J_\Phi \circ M_1$。对于 (U_0, U_1)，欧拉恒等式在 $(0,1)$ 处给出 $\partial_Z U_0(0,1) = d\,a(0) = 0$ 以及 $\partial_Z U_1(0,1) = d\,b(0)$，因此 $J_{(U_0,U_1)}(0,1) = d\,a'(0)\ b(0)$。由于 $M_1(0,1)$ 是 P 的本原代表，且 $v(d) = 2$，这就得到 $\vartheta(P) = v(J(x_0, z_0)) - 2$。根据 (b)，$a'(0) = a_1(0)$ 的赋值为 $\geq 1/e$，并且 $a'(0) = 0$ 当且仅当 $M_2^{-1}\varphi M_1$，等价地说，φ 在 P 处分歧。形式 J 的次数为 $2d-2$，且非零；由于 φ 是可分的，写成 $J = \lambda_J J_0$，其中 $\lambda_J \in K_{\mathfrak{p}}^\times$，并且 J_0 具有单位元系数。约化 $\bar{J}_0 \neq 0$ 在 $\mathbb{P}^1(\mathbb{F}_p)$ 中至多有 $2d-2$ 个零点，而在它们的剩余圆盘之外，$\vartheta = v(\lambda_J) - 2$。□

利用引理 8.1(c)，我们发现每个剩余圆盘中恰有一个周期点。

引理 8.2。每个剩余圆盘 U_ξ 恰好包含一个 η_ξ 周期点 φ。其精确周期为 q_ξ，$\varphi(\eta_\xi) = \eta_{\bar{\varphi}(\xi)}$；如果 $P \in U_\xi$ 不是周期的，则 $w(P, \eta_\xi) = w(\varphi^{q_\xi}(P)\ P)$。

证明。令 $q' = q_\xi$ 和 $G = \varphi^{q'}$。于是 $G(U_\xi) \subseteq U_\xi$，由引理 8.1(c)，对于 $P \neq Q \in U_\xi$，有 $w(G(P)\ G(Q)) > w(P,Q)$；因此 G 在 U_ξ 中至多有一个不动点。为证明存在性，取 $P \in U_\xi$ 并令 $\delta_j = w(G^{j+1}(P)\ G^j(P))$。于是 $\delta_0 > 0$，并且应用引理 8.1(c) q' 次可得，$\delta_{j+1} \geq \rho(\delta_j) \geq \delta_j + \min\{(d-1)\delta_0, 1/e\}$，因此 $\delta_j \to \infty$。由超度量不等式，序列 $G^j(P)$ 是柯西序列；其极限 η 属于闭集 U_ξ，并且是不动点，因为 G 是连续的。对于 $0 < j < q'$，$\varphi^j(\eta)$ 属于 $U_{\bar{\varphi}^j(\xi)} \neq U_\xi$，所以 η 具有精确周期 q'。U_ξ 中的周期点的周期必须被 q' 整除，因为其周期在 $\bar{\varphi}$ 作用下固定 ξ；因此它是某个 $G^j, j \geq 1$ 的不动点，而将上述论证应用于 G^j 可知，它等于 η。点 $\varphi(\eta_\xi)$ 是周期点且属于 $U_{\bar{\varphi}(\xi)}$，因此它等于 $\eta_{\bar{\varphi}(\xi)}$。如果 $P \in U_\xi$ 不是周期的且 $u = w(P, \eta_\xi)$，那么 $w(G(P)\,\eta_\xi) = w(G(P)\ G(\eta_\xi)) > u$，所以 $w(G(P)\ P) = u$。□

因此，$\mathbb{P}^1(\mathbb{C}_p)$ 中 φ 的周期点恰好是点 η_ξ、$\xi \in \mathbb{P}^1(\mathbb{F}_p)$。

在 $K_{\mathfrak{p}}$ 的有限扩张上定义的点的轨道，会以由分歧指数控制的速率趋近于其所在圆盘的周期点的轨道。

引理 8.3。设 $F \subset \mathbb{C}_p$ 是 $K_{\mathfrak{p}}$ 的有限扩张，其绝对分歧指数为 e_F，并令 $m_0 = \lceil \log_d(e_F/e) \rceil \geq 0$。设 $P \in \mathbb{P}^1(F)$ 具有无限轨道，且 $\eta = \eta_{\bar{P}}$。则对所有$n \geq 0$,

$$w\big(\varphi^n(P), \varphi^n(\eta)\big) \;\geq\; \min\{d^n/e_F,\ 1/e\},$$

以及 $w(\varphi^n(P),\ \varphi^n(\eta)) \geq (n - m_0 + 1)/e$ 对于 $n \geq m_0$。

证明。由于 e 整除 e_F，$m_0 \geq 0$。令 $q' = q_{\bar{P}}$。选择坐标位于 F、w 中的本原代表元，则 $\varphi^{q'}(P)$ P 是 F 中某个非零元素的赋值（由于 P 不是周期的，因此该元素非零），且该赋值为正；所以它至少为 $1/e_F$。由引理 8.2，$g_0 = w(P,\ \eta) \geq 1/e_F$。令 $g_n = w(\varphi^n(P)\ \varphi^n(\eta))$；由引理 8.1(c)，$g_{n+1} \geq \rho(g_n)$。由于 ρ 递增，归纳可得 $g_n \geq \min\{d^n/e_F, 1/e\}$：若这对 n 成立，则 $g_{n+1} \geq \min\{d\min\{d^n/e_F, 1/e\},$ $1/e\} \geq \min\{d^{n+1}/e_F, 1/e\}$。由于 $d^{m_0} \geq e_F/e$，$g_{m_0} \geq 1/e$。若 $g \geq 1/e$，则 $dg \geq g + 1/e$，因此 $\rho(g) = g + 1/e$；从而 $g_n \geq (n - m_0 + 1)/e$ 对于 $n \geq m_0$ 成立。□

当没有临界点是周期点时，ϑ 在周期点上有下界，由此得到整数 ν，用于§9。

引理 8.4. 假设 φ 没有临界点是周期的。那么

$$\kappa^* = \sup\{\vartheta(\eta) :\ \eta \ \textit{periodic}\}$$

有限且至少为 $1/e$，因此 $\nu = \lfloor e\kappa^* \rfloor$ 是一个满足 $\nu \geq 1$ 和 $(\nu + 1)/e > \kappa^*$的整数。对于 *Latt`*映射，κ^* 和 ν 仅取决于 E、K 和 $\mathfrak{p}$。

证明。由引理 8.1(d)，$\vartheta \geq 1/e$以及 $\vartheta(\eta_\xi) = \vartheta_0 < \infty$ 除有限多个 ξ之外。对于剩余的有限多个 ξ，η_ξ 是周期的，因此不是临界点，所以 $\vartheta(\eta_\xi) < \infty$。由于周期点恰好是 η_ξ，κ^* 是有限多个有限数中的最大值。□

由引理 7.4、引理 8.4 适用于 Latt`es 映射。

9. 分歧簇与定理 A 的证明

本节将证明，次数的下降会迫使许多共轭元在 $\mathfrak{p}$ 上高度分歧，并利用由此产生的 $\mathfrak{p}$-进簇证明定理 A。

本节中，φ与 §8 中相同，没有周期临界点；κ^*、ν 与引理 8.4 中相同。对于 $\alpha \in \mathbb{P}^1(K)$，我们按 §2 中的记号写作 $\alpha_n = \varphi^n(\alpha)$、$D_n = [K(\alpha_n):\ K]$ 和 $r_n = D_n/D_{n+1}$；若 $r_n \geq 2$，则在第 n 步次数下降。对于 α 的一个 K-共轭元 $x \in \mathbb{P}^1(K) \subset \mathbb{P}^1(\overline{\mathbb{C}_p})$，令 $K_{\mathfrak{p}}(x) \subset \mathbb{C}_p$为由 x 的仿射坐标在 $K_{\mathfrak{p}}$ 上生成的域（其中 $K_{\mathfrak{p}}(\infty) = K_{\mathfrak{p}}$），并令 e_x 为其在 $\mathbb{Q}_p$上的分歧指数。它是 $K(\alpha)$在 $\mathfrak{p}$上方某个素数处的完备化，因此 e_x 至多为 $K(\alpha)$在 $\mathfrak{p}$上方某个素数的最大绝对分歧指数。

9.1. 降阶迫使分歧。我们首先记录 α 的共轭元在 α_n的共轭元上的分布情况。

引理 9.1。设 $\alpha \in \mathbb{P}^1(K)$ 且 $\overline{n} \geq 0$。映射 $x \mapsto \varphi^n(x)$ 将 K-共轭元 α映到 α_n的共轭元上，且纤维恰有 D_0/D_n 个元素；并且 φ 将 K-共轭元 α_n映到 α_{n+1}的共轭元上，且纤维恰有 r_n 个元素。

证明。由于 φ 定义在 K上，这些映射是 $\mathrm{Gal}(K^{-}/K)$-等变的；它们是满射，因为伽罗瓦群在 α_n的共轭元上可传递作用，并且它会传递地置换各纤维，因此它们的大小都相同。□

下一个引理给出一个差商估计：如果周期点η 附近的两个不同点具有相同的像，那么 $\vartheta(\eta)$ 就很大。

引理 9.2。设 $\eta \in \mathbb{P}^1(\mathbb{C}_p)$，并设 $z \neq z'$ 属于 $U_{\bar{\eta}}$ 且满足 $\varphi(z) = \varphi(z')$。则 $\vartheta(\eta) \geq \min\{w(z,\eta)\ w(z',\eta)\}$。

证明。按引理 8.1(b)为 $P = \eta$选取 M_1, M_2，并写作 $z = M_1([t_1 : 1])$、$z' = M_1([t_2 : 1])$；如引理 8.1(c)的证明中那样，$v(t_1) = w(z,\eta) > 0$ 且 $v(t_2) = w(z',\eta) > 0$，并且 $t_1 \neq t_2$。由于 $\varphi(z) = M_2([a(t_1) : b(t_1)])$，$z'$ 也同理，因此我们有 $a(t_1)b(t_2) = a(t_2)b$。多项式

$$\Gamma(\tau_1, \tau_2) = \frac{a(\tau_1)b(\tau_2) - a(\tau_2)b(\tau_1)}{\tau_1 - \tau_2}$$

其系数属于 $\mathcal{O}_{\mathbb{C}_p}$，因为 $\tau_1^i\tau_2^j - \tau_2^i\tau_1^j$在 $\mathbb{Z}[\tau_1, \tau_2]$中可被 $\tau_1 - \tau_2$整除。它满足 $\Gamma(t_1,\ t_2) = 0$且 $\Gamma(0,\ 0) = a'(0)b(0) - a(0)b'(0) = a'(0)b(0)$，其中 $b(0)$是一个单位元。因此 $\vartheta(\eta) = v(\Gamma(0,\ 0) - \Gamma(t_1,\ t_2)) \geq \min\{v(t_1)\ v(t_2)\}$。□

结合前面的引理，我们证明，在第 n 步出现次数下降，会迫使至少一半的 α 共轭元在 $\mathfrak{p}$ 上高度分歧。

引理 9.3。设 α 不是前周期的，并假设在第 n 步出现次数下降。那么集合

$$H_n = \left\{x :\ x \text{ a } K\text{-conjugate of } \alpha \text{ with } e_x > e\, d^{n-\nu}\right\}$$

至少有 $D_0/2$ 个元素。

证明。若 α_n 的某个共轭元 z 满足：存在 α 的某个共轭元 x，使得 $\varphi^n(x) = z$ 具有 $e_x \leq e\, d^{n-\nu}$，则称 z 为坏的。由于 e 整除 e_x，当 $n < \nu$ 时，不存在坏的元素。

我们断言，φ 在 α_n 的共轭元上的每个纤维至多包含一个坏的元素。假设某个纤维中的 $z \neq z'$ 是坏的，其中 x、x' 如定义所述。那么 $\varphi(z) = \varphi(z')$，因此$\bar{z} = \bar{z}'$，因为 $\bar{\varphi}$ 是单射（引理 8.1(a)）；令 η 为该剩余圆盘的周期点。由于$\bar{\varphi}^n(\bar{x}) = \bar{z}$，引理 8.2 给出 $\varphi^n(\eta_{\bar{x}}) = \eta$。设 $m_0 = \lceil \log_d(e_x/e) \rceil$。由于 $e_x/e \leq d^{n-\nu}$ 且 $n - \nu$是整数，$0 \leq m_0 \leq n - \nu$；再将引理 8.3 应用于满足 $F = K_{\mathfrak{p}}(x)$的 x，得到

$$w(z,\eta) \geq \frac{n - m_0 + 1}{e} \geq \frac{\nu + 1}{e} > \kappa^*.$$

同样 $w(z',\ \eta)\ >\kappa^*$。由引理 9.2，$\vartheta(\eta)\ >\kappa^*$，这与 κ^* 的定义矛盾。

由引理 9.1 可知，纤维具有 $r_n\geq 2$ 个元素，因此至少有 $(1-1/r_n)D_n\geq D_n/2$ 个 α_n 的共轭元不是坏的，而 D_0/D_n 的共轭元 α 在它们各自上方的共轭元均位于 H_n中。□

9.2. **共轭元簇**。一个分歧指数为 e_x 的共轭元位于一个由 e_x/e 个共轭元组成的簇中，其轨道保持 $\mathfrak{p}$-进接近。

引理 9.4。设 α 不是前周期的，x 是 α 的 K-共轭元，且 $K_x^{\mathrm{ur}}\subseteq K_{\mathfrak{p}}(x)$ 是 $K_{\mathfrak{p}}$ 在 $K_{\mathfrak{p}}(x)$ 中的最大非分歧扩张。由 $\mathcal{C}(x)$ 组成的 x 在 K_x^{ur} 上的共轭元集合包含 e_x/e 个 α 的共轭元，并且

$$w\big(\varphi^n(x'),\varphi^n(x'')\big)\ \geq\ \min\{d^n/e_x,\ 1/e\}\qquad \textit{for } x'\neq x''\ \textit{in}\ \mathcal{C}(x)\ \textit{and}\ n\geq 0.$$

证明。如果 $x=\infty$，则 $\mathcal{C}(x)=\{x\}$，无需证明；设 $x\neq\infty$。集合 $\mathcal{C}(x)$ 具有 $[K_{\mathfrak{p}}(x)\colon K_x^{\mathrm{ur}}]=e_x/e$ 个元素，它们都是 α 在 K 上的最小多项式的根。对于 $x'\in\mathcal{C}(x)$，K_x^{ur}-同构 $K_x^{\mathrm{ur}}(x)\to K_x^{\mathrm{ur}}(x')$ 是等距的，因为 K_x^{ur} 是完备的；因此 $K_{\mathfrak{p}}(x')=K_x^{\mathrm{ur}}(x')$ 的分歧指数为 e_x。由于 $K_{\mathfrak{p}}(x)$ 与 K_x^{ur} 具有相同的剩余域，存在 $t\in\mathbb{P}^1(K_x^{\mathrm{ur}})$，使得 $w(x,t)>0$，进而 $w(x',t)=w(x,t)>0$。所以 $\mathcal{C}(x)$ 位于一个剩余圆盘 U_ξ 中。对每个满足 $F=K_{\mathfrak{p}}(x')$ 的 $x'\in\mathcal{C}(x)$ 应用引理 8.3，并结合相同的 $\eta=\eta_\xi$ 和超度量不等式，即得所述结论。□

9.3. **最后一次次数下降时的能量**。我们沿用 §6中的记号：格林函数 g_ι、集合 $\mathcal{S}$（赋值集）、性质 (G1)–(G4) 以及常数 C 和 $\lambda_{\mathfrak{p}}$。

现在，我们用 $\mathfrak{p}$ 处 α_m 的共轭元的能量给 $h_\varphi(\alpha)$ 取一个下界，其中 m 是次数下降的一步。

命题 9.5。设 α 不是前周期的，并假设次数在第 m 步下降。那么

$$\widehat{h}_\varphi(\alpha)\ \geq\ \frac{\lambda_{\mathfrak{p}}}{4d^\nu D_0}-\frac{e\lambda_{\mathfrak{p}}+2C\log D_m}{4D_m\,d^m}.$$

证明。设 S 为 $N=D_m$ 的 α_m共轭元集合；由于次数在第 m 步下降，$N\geq r_m\geq 2$。设 L' 是 K 的一个有限 Galois 扩张，在该扩张上 S 的各点均有定义。对于嵌入 σ，从 L'写作 $g_\sigma(\beta,\beta')=g_{\sigma|_K}(\sigma\beta,\sigma\beta'$。证明沿用命题 6.2的思路：以单个层级 S代替 $S_0\cup\cdots\cup S_k$，

$$\sum_{\sigma}\sum_{\beta\neq\beta'\in S}g_\sigma(\beta,\beta')\ =\ 2(N-1)\,[L':\mathbb{Q}]\,N\,\widehat{h}_\varphi(\alpha_m)\ \leq\ 2[L':\mathbb{Q}]\,N^2d^m\,\widehat{h}_\varphi(\alpha),$$

在 $\mathcal{S}$ 中诱导出赋值的嵌入至少贡献 $-[L'\colon\ \mathbb{Q}]\,C\,N\log\ N$，而所有其他嵌入的贡献至少为 0。

σ 是以下 $[L'$ 之一：将 $L'\ \ K]\,ef$ 嵌入 $\mathbb{C}_p$ 并在 K上诱导 $\mathfrak{p}$ 的g_σ嵌入。根据（G2），$\beta,\ \beta'$的 $=w(\sigma\beta,\ \sigma\beta')$为 $\log\ p$。σ对 K的限制与 K的固定嵌入都可延拓为将 $K_{\mathfrak{p}}$ 嵌入 $\mathbb{C}_p$的 $\mathbb{Q}_p$-嵌入，因此二者相差一个 $\mathbb{C}_p$的连续自同构 θ，而该自同构保持 v不变；于是 $\theta^{-1}\circ\sigma$ 与固定嵌入在 K 上一致，因此它们在 L' 上相差一个

Gal(L'/K)中的元素，该元素置换 S。因此，$\sum_{\beta\neq\beta'\in S} w(\sigma\beta,\ \sigma\beta')$等于其在固定嵌入下的值 $\mathcal{G}$。

由引理 9.3，$|H_m|\geq D_0/2$。设 $x\in H_m$ 和 $y=\varphi^m(x)$。由引理 9.4 和 9.1，集合 $\varphi^m(\mathcal{C}(x))\subseteq S$ 包含 y 以及至少 $(e_x/e)\,N/D_0$ 个两两之间的弦度量赋值为$\geq\delta_x=\min\{d^m/e_x,1/e\}\leq 1$的点。由于 $e_x>e\,d^{m-\nu}$，点 y对 $\mathcal{G}$至少有贡献

$$\Big(\frac{e_xN}{eD_0}-1\Big)\delta_x\ \geq\ \frac{N}{D_0}\min\Big\{\frac{d^m}{e},\ \frac{e_x}{e^2}\Big\}-1\ \geq\ \frac{d^{m-\nu}N}{eD_0}-1.$$

至少有 $|H_m|N/D_0\geq N/2$ 个这样的点 y，因此 $\mathcal{G}\geq\frac{N}{2}\big(\frac{d^{m-\nu}N}{eD_0}-1\big)$（如果括号内为负，则使用 $\mathcal{G}\geq 0$）。合并并除以 $[L'\colon\ \mathbb{Q}]$，由于 $[L'\colon\ K]ef\log p/[L'\colon\ \mathbb{Q}]=e\lambda_{\mathfrak{p}}$,

$$2N^2d^m\,\widehat{h}_\varphi(\alpha)\ \geq\ e\lambda_{\mathfrak{p}}\mathcal{G}-CN\log N\ \geq\ \frac{\lambda_{\mathfrak{p}}d^{m-\nu}N^2}{2D_0}-\frac{e\lambda_{\mathfrak{p}}N}{2}-CN\log N,$$

这就是要证明的结论。 □

9.4. **定理 A的证明**。

定理 A 的证明。令 $k(D)$、c_1'、c_2 和 $\mathcal{B}$ 如定理 2.1 中所述，对应于 Latt`es 映射 φ；由引理 7.4 可知，该映射没有周期临界点。设 $c_4=\lambda_{\mathfrak{p}}/(4d^\nu)$，并令 $c_5=\max\{1,\,e\lambda_{\mathfrak{p}}/4+C/2\}$，使得对所有 $N\geq 1$，$(e\lambda_{\mathfrak{p}}+2C\log N)/4\leq c_5\log 3N$。取非挠点 P，$\alpha=x(P)$；由引理 7.3 可知，它不是前周期点，$D=D_0$ 并且 $X_D=\exp(-c_2\sqrt{\log 3D})$，使得 $\mathcal{B}(D)=c_1'X_D/D$。回忆 $\widehat{h}_E(P)=\frac{1}{2}\widehat{h}_\varphi(\alpha)$。

如果次数从未下降，定理 2.1 结合 $m=0$ 可得 $h_\varphi(\alpha)\geq c_1'X_D/D$，这意味着 (i) 和 (ii) 均成立。否则，由于 (D_n) 是一个非递增的正整数序列，因此存在最后一个次数下降的步骤 m，将定理 2.1 中的 $m+1$ 替换为 m应用后可得

$$\widehat{h}_\varphi(\alpha)\ \geq\ \frac{c_1'X_D}{D}\prod_{n\leq m}\frac{r_n}{d}\ =\ \frac{c_1'X_D}{D_{m+1}\,d^{m+1}}. \tag{8}$$

对于 (i)：由引理 9.3，存在 α 的一个共轭元 x，使得 $e\,d^{m-\nu}<e_x$；又因为 $K(\alpha)\subseteq K(P)$，所以 $e_x\leq e_{\mathfrak{p}}(P)$；因此 $d^{m+1}<d^{\nu+1}e_{\mathfrak{p}}(P)/e\leq d^{\nu+1}e_{\mathfrak{p}}(P)$，并且将 $D_{m+1}\leq D$ 代入 (8) 可得 $\widehat{h}_\varphi(\alpha)\geq c_1'd^{-\nu-1}X_D/(e_{\mathfrak{p}}(P)D)$。

对于 (ii)：由 (8) 和 $D_{m+1}\leq D_m$，我们有 $h_\varphi(\alpha)\geq(c_1'/d)X_D/(D_md^m)$。若 $c_4/D\geq 2c_5\log(3D_m)/(D_md^m)$，则由命题 9.5 得 $h_\varphi(\alpha)\geq c_4/(2D)$。否则 $D_md^m<(2c_5/c_4)D\log 3D$，并且

$$\widehat{h}_\varphi(\alpha)\ \geq\ \frac{c_1'c_4}{2c_5d}\cdot\frac{X_D}{D\log 3D}.$$

当 $X_D\leq 1\leq\log 3D$ 和 $e_{\mathfrak{p}}(P)\geq 1$时，两部分都以定理 c_2 的常数 2.1 成立，并且

$$c_1=\tfrac{1}{2}\min\big\{c_1'd^{-\nu-1},\ c_4/2,\ c_1'c_4/(2c_5d)\big\}.$$ □

10. Points of bounded residue degree

本节证明定理 B； Φ 和 φ 是第 §7 节中的 Lattes 对和映射。证明既不使用增长同余，也不使用定理 2.1。我们只用到 $[p]$ 在 $\mathfrak{p}$-进意义下压缩形式群，并且 P 的共轭元落在有限个剩余类中，然后比较轨道中一对相邻层级。

10.1. **形式群**。 我们沿用嵌入 $K \hookrightarrow \mathbb{C}_p$ 和赋值 v，取自 §8。我们使用以下事实，它们对每个包含 $\subseteq \mathbb{C}_p$ 的闭子域 Ω $K_{\mathfrak{p}}$均成立，其中 $\mathfrak{m}_\Omega$ 是其赋值环的极大理想。设 E 为 E的形式群，参数为 $t = -x/y$；其群 law、逆元以及级数 $[m](T)$ 的系数属于 $\mathcal{O}$ [16, IV.1–IV.2]。

(F1) 约化是一个满同态 $E(\mathbb{C}_p) \to \widetilde{E}(\mathbb{F}_p)$。其核 E^1 由 O以及满足 $v(x) < 0$ 的点组成，并且 $R \mapsto t(R)$ 是从 $E^1(\Omega)$ 到 $\widehat{E}(\mathfrak{m}_\Omega)$ 的同构；对于 $R \in E^1$, $R \neq O$，有 $v(x(R)) = -2v(t(R))$。这是 [16, VII.2.1、VII.2.2]； $\mathbb{C}_p$ 上的满射性由 VII.2.1 应用于 $K_{\mathfrak{p}}$的有限非分歧扩张可得，因为 $E(\mathbb{F}_p)$ 中的每个点都定义在有限域上。

（F2）对于 $R, R' \in E^1$, $v(t(R - R')) \geq \min\{v(t(R)) \; v(t(R'))\}$，因为 $t(R - R')$ 是 $t(R)$ $t(R')$ 上的幂级数，系数属于 $\mathcal{O}$，且常数项为零。
（F3）对于与 p 互素的 m， $[m](T) = mT + \cdots$，所以 $[m]$ 是 $E^1(\Omega)$ [16, IV.2.3] 的自同构。
（F4）由于 $\widetilde{E}$ 是超奇异的， $\widehat{E}$ 的高度为 2 [16, V.3.1],，因此对于某个 $h_0 \in k[[T]]$ [16, IV.7.2]，有 $[p](T) \equiv h_0(T^{p^2})$（模 $\mathfrak{p}$）。于是 $[p](T) = \sum_{i \geq 1} a_i T^i$，其中 $a_1 = p$、 $a_i \in \mathfrak{p}$ 对于 $1 \leq i < p^2$，且 $a_{p^2} \in \mathcal{O}^\times$。置

$$\varepsilon_E = \min_{1 \leq i < p^2} v(a_i), \qquad \frac{1}{e} \leq \varepsilon_E \leq 1, \qquad \rho_E(s) = \min\{p^2 s, \; s + \varepsilon_E\}.$$

于是，对于 $R \in E^1$，有 $v\big(t([p]R)\big) \geq \rho_E\big(v(t(R))\big)$。

对于 (F4)：如果 $s = v(t(R)) > 0$，则含有 $i < p^2$ 的项的赋值至少为 $\varepsilon_E + is \geq s + \varepsilon_E$，其余项的赋值至少为 $p^2 s$。

$E(\mathbb{C}_p)$的每个剩余类都包含一个阶与 p互素的典范挠点，它发挥着剩余圆盘的周期点的作用。

引理 10.1。 $E(\mathbb{C}_p)$ 的每个剩余类 $R + E^1$ 都恰好包含一个阶与 p互素的挠点，记为 $\omega(R)$。映射 $R \mapsto \omega(R)$ 是一个同态；如果 $R \in E(\Omega)$，那么 $\omega(R) \in E(\Omega)$。

证明。 由于 E 是超奇异的，$E(\mathbb{F}_p)$没有阶为 p [16, V.3.1], 的点，因此 R 的阶与 p互素。于是 $[m]R \in E^1$；根据 (F3)，存在唯一的 $z \in E^1$ 满足 $[m]z = [m]R$；点 $\omega = R - z$ 满足 $[m]\omega = O$。同一剩余类中的两个阶与 p 互素的挠点之差是 E^1 中一个阶与 p互素的点，根据 (F3)，该点为 O。如果 $R \in E(\Omega)$，则根据 (F3)， $[m]R \in E^1(\Omega)$且 $z \in E^1(\Omega)$，因此 $\omega \in E(\Omega)$。同态性质由唯一性得出。□

下一个引理量化了形式群在 $[p]$ 下的收缩。

引理 10.2. 设 $e' \geq 1$，并令 $j_0 \geq 0$ 为满足 $p^{2j_0} \geq \varepsilon_E e'$ 的最小整数。令 $u_0 = 1/e'$ 和 $u_{j+1} = \rho_E(u_j)$。则 (u_j) 是递增的，并且对 $j \geq j_0$ 有 $u_j \geq \varepsilon_E(j - j_0 + 1)$。

证明。由于 $\rho_E(s) > s$ 对 $s > 0$而言是递增的，(u_j) 也是递增的。令 $a > 0$ 和 $b = \min\{a, \varepsilon_E\}$。若 $s \geq b$，那么由于 ρ_E 是递增的，

$$\rho_E(s) \geq \rho_E(b) = \min\{p^2 b,\ b + \varepsilon_E\} \geq \min\{p^2 a,\ \varepsilon_E\};$$

由归纳法可得 $u_j \geq \min\{p^{2j}/e', \varepsilon_E\}$，因此 $u_{j_0} \geq \varepsilon_E$。对于 $s \geq \varepsilon_E$，我们有 $p^2 s \geq s + \varepsilon_E$，所以$\rho_E(s) = s + \varepsilon_E$，结论由归纳法得出。□

10.2. **局部高度**。对于数域 σ 的一个嵌入 $L' \supseteq K$ 到某个 $\mathbb{C}_\ell$ 以及 β中，$\beta' \in \mathbb{P}^1(L')$ 置 $g_\sigma(\beta, \beta') = g_{\sigma|_K}(\sigma\beta,\ \sigma\beta')$，其中 g_ι 如 §6中所述，并且 $\infty = (1:0) = x(O)$。

我们汇总证明中所使用的格林函数的性质。

引理 10.3。(a) 对于 $R \in E(L'),\quad R \neq O,\quad \frac{1}{2}\sum_\sigma g_\sigma(x(R)\ \infty) = [L':\ \mathbb{Q}]\,\widehat{h}_E(R)$。

(b) 对于每个将 K 嵌入到某个 $\mathbb{C}_\ell$ 中的嵌入 ι，存在 $b_\iota \geq 0$，使得对于所有 $w \neq 0$，$\big|\log \|\Phi^\iota(w)\| - d\log \|w\|\big| \leq b_\iota$。令 $a_\iota = 0$，如果 ι 在 $\mathcal{S}$之外诱导出一个赋值；若 ι 是阿基米德的，则 $a_\iota = \log 2 + 2b_\iota/(d-1) + |r_\iota|$；否则令 $a_\iota = 2b_\iota/(d-1) + |r_\iota|$。那么对于所有不同的 z、$z' \in \mathbb{P}^1(\mathbb{C}_\ell)$，$g_\iota(z, z') \geq -a_\iota$。

(c) 若 σ 诱导出 $\mathcal{S}$之外的赋值，则 $g_\sigma(x(R)\ \infty) = \log^+ |x(R)|_\sigma$，其中 $\log^+ = \max\{0, \log\}$。若 $\sigma\colon\ L' \hookrightarrow \mathbb{C}_p$ 延拓了 K 和 $\sigma R \in E^1$的固定嵌入，则$\frac{1}{2} g_\sigma(x(R)\ \infty) = v\big(t(\sigma R)\big)\log p$。

固定 b_ι，令 $C_{\mathrm{bad}} = [K:\ \mathbb{Q}]^{-1}\sum_\iota a_\iota$；它是有限的，且 $C_{\mathrm{bad}} \geq \log 2$。

证明。(a) 取提升 $(x(R), 1)$ 和 $(1, 0)$，其楔积为 -1。将定义对$\sim\sigma$求和，乘积公式和 $\mathrm{Res}(\Phi) \in K^\times$ 给出 $\sum_\sigma r_\sigma = 0$，而 (G3) 给出 $[L':\ \mathbb{Q}](h_\varphi(x(R)) + h_\varphi(\infty))$。由于 $\Phi(1, 0) = (1, 0)$，$h_\varphi(\infty) = 0$，并且根据引理 7.3，$h_\varphi(x(R)) = 2h_E(R)$。(b) 由三角不等式可得 $\log \|\Phi^\iota(w)\| - d\log \|w\|$ 的上界；下界则来自将 $\mathrm{Res}(\Phi)X^{2d-1}$ 和 $\mathrm{Res}(\Phi)Z^{2d-1}$ 表示为 Φ_0、Φ_1的多项式系数组合的恒等式；由此得到 b_ι。在 $\mathcal{S}$ 之外，结论就是 (G2)。一般而言 $g_\iota = -\log \frac{|\tilde{z}\wedge\tilde{z}'|}{\|\tilde{z}\|\|\tilde{z}'\|} + (\widehat{H}_\iota - \log\|\cdot\|)(\tilde{z}) + (\widehat{H}_\iota - \log\|\cdot\|)(\tilde{z}') - r_\iota$。若 ι 是阿基米德的，则第一项为 $\geq -\log 2$，否则为 ≥ 0；而对于 $G = \Phi^\iota$，

$$\widehat{H}_\iota(w) - \log\|w\| = \sum_{j\geq 0} d^{-j-1}\Big(\log\|G^{(j+1)}(w)\| - d\log\|G^{(j)}(w)\|\Big)$$

绝对值至多为 $b_\iota/(d-1)$。最后，由于 $\mathcal{S}$ 是有限的，C_{bad} 也是有限的，并且由于存在 $[K$ 个阿基米德嵌入，$C_{\mathrm{bad}} \geq \log 2:\ \mathbb{Q}]$。(c) 根据 (G2)，$g_\sigma(x(R)\ \infty) = -\log\big(1/\max\{|x(R)|_\sigma,\ 1\}\big) = \log^+|x(R)|_\sigma$。如果 σ 延拓了固定嵌入，则 $|x(R)|_\sigma = p^{-v(x(\sigma R))}$，而 (F1) 给出 $\log^+|x(R)|_\sigma = 2v(t(\sigma R))\log p$ for $\sigma R \in E^1$。□

10.3. **定理 B的证明**。设 P为非挠元，$D' = [K(P):\ K]$，P_1，……，$P_{D'}$是 K的 P个共轭元，视为 $E(\mathbb{C}_p)$ 中的元素，$e' = e_{\mathfrak{p}}(P)$，并且 $L' \subset K$ 是$\overline{K}$ 的一个有限 Galois 扩张，在该扩张上所有 P_i 都有定义。

$K(P)$ 中位于 $\mathfrak{p}$ 之上的每个素数的剩余次数至少为 f，因此不妨设 $f_0 \ge f$。令 $U \subset E(\mathbb{F}_p)$ 为所有满足 $j \le f_0$ 被 f 整除的群 $E(\mathbb{F}_{p^j})$ 的并，令 $N_0 = |U|$，令 μ_0 为由 U 生成的有限群的指数，该指数与 p 互素，并令 $\kappa_0 \ge 1$ 为 p 模 μ_0 的阶。所有这些量只依赖于 E、$\mathfrak{p}$ 和 f_0。令 Ω_i 为 $K_{\mathfrak{p}}(P_i)$ 在 $\mathbb{C}_p$ 中的闭包；它是 $K(P_i) \cong K(P)$ 在 $\mathfrak{p}$ 之上的某个素数处的完备化，因此其绝对分歧指数 e_i 至多为 e'，且其剩余域包含 k，其次数至多为 f_0 在 $\mathbb{F}_p$ 上的次数。因此 $P_i \in U$。

令 $\omega_i = \omega(\bar{P}_i)$ 和 $z_i = P_i - \omega_i$。由引理 10.1，$\omega_i \in E(\Omega_i)$，因此 $z_i \in E^1(\Omega_i)$，并且 $z_i \neq O$，因为 P 不是挠点。因此 $t(z_i)$ 是 Ω_i 中的一个具有正赋值的非零元素，所以 $v(t(z_i)) \ge 1/e_i \ge 1/e'$。由 (F4) 以及 ρ_E 递增可知，对于所有 $j \ge 0$，都有 $v\big(t([p^j]z_i)\big) \ge u_j$，其中 u_j 如引理 10.2 所述。

固定 $n \ge 0$，令 $m = n + \kappa_0$ 和 $R_{ii'} = [p^n]P_i - [p^m]P_{i'} \in E(L')$。若 $R_{ii'} = O$，则 $[p^n]P$ 和 $[p^m]P$ 在 K 上互为共轭元，因此 $p^{2n}\widehat{h}_E(P) = p^{2m}\widehat{h}_E(P)$ 和 P 将是挠点；于是 $R_{ii'} \neq O$。由引理 10.3(a) 及平行四边形定律，

$$\mathcal{E} = \frac{1}{2}\sum_{\sigma}\sum_{i,i'} g_\sigma\big(x(R_{ii'}),\infty\big) = [L':\mathbb{Q}]\sum_{i,i'}\widehat{h}_E(R_{ii'}) \;\le\; 2[L':\mathbb{Q}]\,D'^2\,(p^{2n}+p^{2m})\,\widehat{h}_E(P). \tag{9}$$

根据引理 10.3(b)，σ 诱导 $\mathcal{S}$ 的赋值至少贡献 $-\frac{1}{2}D'^2[L':K]\sum_\iota a_\iota = -\frac{1}{2}[L':\mathbb{Q}]D'^2C_{\mathrm{bad}}$；根据 (G2)，其他 σ 贡献非负项。令 $\sigma\colon L' \hookrightarrow \mathbb{C}_p$ 在 K 上诱导 $\mathfrak{p}$；这样的 $[L':K]\,[K_{\mathfrak{p}}:\mathbb{Q}_p] = [L':K]\,ef$ 共有。σ 到 K 的限制以及 K 的给定嵌入，都可延拓为 $\mathbb{Q}_p$ 到 $K_{\mathfrak{p}}$ 的嵌入，它们相差 $\mathrm{Gal}(\mathbb{Q}_p/\mathbb{Q}_p)$ 的一个元素；通过连续性将其延拓，得到 $\mathbb{C}_p$ 的一个自同构 θ，满足 $v\circ\theta = v$ 以及在 L' 上 $\sigma = \theta\circ\gamma$，其中 $\gamma \in$ 属于 $\mathrm{Gal}(L'/K)$。于是，$|x(R)|_\sigma = |\theta(x(\gamma R))|_p = |x(\gamma R)|_p$，并且 $\gamma R_{ii'} = R_{\gamma i,\,\gamma i'}$，其中 $\gamma P_i = P_{\gamma i}$。因此，根据引理 10.3(c)，

$$\frac{1}{2}\sum_{i,i'} g_\sigma\big(x(R_{ii'}),\infty\big) = \frac{1}{2}\sum_{i,i'}\log^+\big|x(R_{ii'})\big|_p,$$

其中右侧的 $R_{ii'}$ 通过固定嵌入视为 $E(\mathbb{C}_p)$ 中的元素。假设 $P_i = P_{i'}$，则 $\omega_i = \omega_{i'} =: \omega$。由于 ω 属于群 $\omega(G)$，其中 G 由 U 生成，因此 $R_{ii'} = [p^n]z_i - [p^m]z_{i'} \in E^1$。由 (F2) 和引理 10.2，$v(t(R_{ii'})) \ge \min\{u_n,u_m\} = u_n$，故根据引理 10.3(c)，$(i,\,i')$ 的项至少为 $u_n\log p$。其他项均非负。由于 $\bar{P}_i$ 属于 U，根据柯西 – 施瓦茨不等式，满足 $\bar{P}_i = \bar{P}_{i'}$ 的有序对数量至少为 D'^2/N_0。因此

$$\mathcal{E} \;\ge\; [L':K]\,ef\log p\cdot\frac{D'^2}{N_0}\,u_n \;-\; \frac{1}{2}[L':\mathbb{Q}]\,D'^2\,C_{\mathrm{bad}}.$$

取 $\Lambda = N_0[K:\mathbb{Q}]/(ef\log p)$，与 (9) 比较并除以 $[L':\mathbb{Q}]D'^2$，

$$\frac{u_n}{\Lambda} \;\le\; \frac{C_{\mathrm{bad}}}{2} + 4p^{2(n+\kappa_0)}\,\widehat{h}_E(P) \qquad \text{for every } n \ge 0.$$

取 $n = j_0 - 1 + \lceil \Lambda C_{\mathrm{bad}}/\varepsilon_E\rceil$，其中 j_0 如引理 10.2中所述；于是 $n \ge j_0$，且 $u_n \ge \varepsilon_E\lceil\Lambda C_{\mathrm{bad}}/\varepsilon_E\rceil \ge \Lambda C_{\mathrm{bad}}$，因此 $4p^{2(n+\kappa_0)}\widehat{h}_E(P) \ge C_{\mathrm{bad}}/2$。由 j_0 的最小性，$p^{2(j_0-1)} < \varepsilon_E e' \le$

e' 若 $j_0 \geq 1$，且 $p^{2(j_0-1)} < 1 \leq e'$ 若 $j_0 = 0$。利用 $\varepsilon_E \geq 1/e$,

$$\widehat{h}_E(P) \;\geq\; \frac{C_{\mathrm{bad}}}{8\,p^{2\kappa_0+2\lceil e\Lambda C_{\mathrm{bad}}\rceil}} \cdot \frac{1}{e'} =: \frac{c_3}{e_{\mathfrak{p}}(P)}.$$

最后 $e_{\mathfrak{p}}(P) \leq e[K(P)\colon K] \leq 2eD$。 □

注 10.4（最优性）。定理 B 中 $e_{\mathfrak{p}}(P)$ 的指数不能降低。设$Q_0 \in E(K) \cap E^1$ 是一个非挠点，且 $v_{\mathfrak{p}}(t(Q_0)) = 1$，并令 $n \geq 1$。由 (F4)，$[p](T) \equiv h_0(T^{p^2})$（模 $\mathfrak{p}$），其中 $h_0(T) = \bar{a}_{p^2}T + \cdots$，$\bar{a}_{p^2} \neq 0$；迭代可得，$[p^n](T)$ 的次数低于 p^{2n} 的项的系数属于 $\mathfrak{p}$，而次数为 p^{2n} 的项的系数是一个单位元，因此由魏尔斯特拉斯预备定理，$[p^n](T) - t(Q_0)$ 是一个次数为 p^{2n}、系数属于 $\mathcal{O}_{K_{\mathfrak{p}}}$ 的艾森斯坦多项式乘以一个单位元。它的根是 $[p^n]^{-1}(Q_0)$ 中 p^{2n} 个点的取值 $t(P)$，这些取值全都属于 E^1。因此，每个$P \in [p^n]^{-1}(Q_0)$ 都有 $[K(P)\colon K] = p^{2n}$，在 $\mathfrak{p}$ 上方有一个素数，且在 $\mathfrak{p}$ 上完全分歧，所以$e_{\mathfrak{p}}(P) = ep^{2n}$，剩余次数为 f，并且 $\widehat{h}_E(P) = \widehat{h}_E(Q_0)p^{-2n} = e\,\widehat{h}_E(Q_0)/e_{\mathfrak{p}}(P)$。这里 $p^{2n}/2 \leq D \leq p^{2n}$ 也成立，因此 $\widehat{h}_E(P) \leq \widehat{h}_E(Q_0)/D$，定理 A 中的指数 1 同样是最优的。这样的 Q_0 确实存在：例如 $E\colon y^2 + y = x^3 - x$ 在 $\mathbb{Q}$ 上，它在$\sim p = 3$、17 和 19 处是超奇异的，且 $n_p = |E(\mathbb{F}_p)| = 7$、18、20；点 $Q_0 = [n_p](0,0)$ 是非挠点，并且在每种情况下都满足 $v_p(t(Q_0)) = 1$。

11. Supersingular primes over number fields

本节记录已知何时存在良好超奇异约化素数；定理A–C 只需一个。

对于具有复乘的曲线，以及其 j-不变量生成一个具有实嵌入的域的曲线，这类素数均存在。

命题 11.1。设 E 是数域 K上的椭圆曲线。那么，E 在以下每种情形下都有无穷多个良好超奇异约化素数：

(a) E 具有复乘；(b)域 $\mathbb{Q}(j(E))$ 具有实嵌入；特别地，E 定义在具有实嵌入的域上，或者 $j(E) \in \mathbb{Q}$。

证明。在良约化素数 $\mathfrak{Q}$ 处的约化是否为超奇异，只取决于 $j(E)$ 模 $\mathfrak{Q}$，因为超奇异性是约化曲线在剩余域 [16, V.3.1]的代数闭包上的性质。此外，E 仅在有限多个素数处具有坏约化。

(a) 设 E 具有由虚二次域 F_0中的某个阶给出的复乘。根据 Deuring 判据 [11, 第 13], 章，在惰性于 F_0 的有理素数上方的良约化素数处，其约化为超奇异。这样的有理素数有无穷多个。

(b) 令 $K_0 = \mathbb{Q}(j(E))$。存在一条椭圆曲线 E_0/K_0，满足 $j(E_0) = j(E)$ [16, III.1.4]。由于K_0 具有实嵌入，Elkies [7] 证明了 E_0 具有无穷多个超奇异约化素理想。在 K 上位于此类素理想之上的每个素理想 $\mathfrak{Q}$ 处，只要 E 和 E_0 都具有良约化

， $j(E)$ 模 $\mathfrak{Q}$ 是一个超奇异的 j-不变量，因此 E 在$\mathfrak{Q}$处具有超奇异约化。□

对于 E 没有复乘且 $\mathbb{Q}(j(E))$ 完全复的情形，一般而言尚不知道超奇异素数是否存在；在具体情况下，通常可以通过计算找到。例如，在 $K=\mathbb{Q}(i)$ 上，曲线 $y^2+y=x^3+ix$ 和 $y^2=x^3+ix+1$的 j-不变量分别为 $110592(64-27i)/4825$ 和 $-6912i(27+4i)/745$，它们既非实数也非整数，并且分别在 $(1+i)$ 和 (3) 处具有良好超奇异约化。

12. Abelian varieties isogenous to products

在本节 中我们证明定理 C，并给出其适用于阿贝尔簇的例子 s.

设 A 是定义在 K上的阿贝尔簇。我们使用丰对称线丛 $\mathcal{L}$ [10, §B.5]的 N´eron–Tate 高度$\widehat{h}_{A,\mathcal{L}}$ 的以下性质：它非负，并且恰好在$\widehat{}$挠点处为零；它在对称线丛上关于 $\mathcal{L}$ 具有可加性；对于同态 $\phi\colon A\to B$，有 $h_{B,\mathcal{M}}(\phi(P))=h_{A,\phi^*\mathcal{M}}(P)$；以及对于 $B=E_1\times\cdots\times E_g$和 $\mathcal{M}=\bigotimes_i \mathrm{pr}_i^*\mathcal{O}_{E_i}(O_i)$，

$$\widehat{h}_{B,\mathcal{M}}(Q_1,\dots,Q_g) \;=\; \sum_{i=1}^{g}\widehat{h}_{E_i}(Q_i),$$

$\widehat{}$其中， h_{E_i} 是 $\mathcal{O}_{E_i}(O_i)$的 N´eron–Tate 高度，即本文其余部分所采用的高度。由于 $A(K)$上的这些高度与定义域无关，我们可以将基域扩张至 K'后再计算它们。

下一个 引理比较两个丰对称线丛的 N´eron–Tate 高度 s.

$\widehat{}$**引理 12.1. </style}设 、是上的丰对称线丛。存在，使得，** $\mathcal{L}'\le_{\wedge} n\,h_{A,\mathcal{L}}$ 在 $A(K)$ *</style}*上。

证明。 *</style}*当 充分大时，是丰的，并且是对称的。因此，其 *Neron–Tate* 高度非负，并且根据可加性，它等于，$\mathcal{L}-h_{A,\mathcal{L}'}$。□

定理 *C*的证明。 *</style}*将替换为的伽罗瓦闭包后，不妨设是伽罗瓦的：同源仍然有定义，并且在所选素数上方的素数处保持良好超奇异约化。设：是该同源，且如上。于是是丰的，因为是有限的；并且是对称的，因为 与交换。由引理 *12.1*$\widehat{}$存在 n，使得 $h_{A,\phi^*\mathcal{M}}\le n\,h_{A,\mathcal{L}}$，因此

$$\widehat{h}_{A,\mathcal{L}}(P) \;\ge\; \frac{1}{n}\widehat{h}_{B,\mathcal{M}}(\phi(P)) \;=\; \frac{1}{n}\sum_{i=1}^{g}\widehat{h}_{E_i}(Q_i),\qquad (Q_1,\dots,Q_g)=\phi(P).$$

若 P不是挠点，则 $\phi(P)$ 也不是挠点，因为 $\ker\phi$ 是有限的；因此存在某个 Q_i 不是挠点。由于 ϕ 定义在 K'上，点 Q_i 定义在 $K'(P)$上，因此 $D_i=[K'(x(Q_i))\colon K']$ 整除 $[K'(P)\colon K']$。由于 K'/K是伽罗瓦扩张，$[K'(P)\colon K']=[K(P)\colon K(P)\cap K']$，它整除 D_i。于是 $D_i\le D$。对 K' 上的 E_i应用定理 A(ii)，得到 $\widehat{h}_{E_i}(Q_i)\ge c_{1,i}D_i^{-1}(\log 3D_i)^{-1}\exp(-c_{2,i}\sqrt{\log\,3D_i})$，且右侧随 D_i增大而减小；因此取 $c=\min_i c_{1,i}/n$ 和 $c'=\max_i c_{2,i}$时，结论成立。□

定理C 的假设在以下情形下成立。

推论 12.2。 定理C 的结论在以下每种情况下均成立：

(a) A 在 K 上同源于椭圆曲线 E_i 在 K上的乘积，其中每条曲线都具有复乘，或者 $\mathbb{Q}(j(E_i))$ 具有实嵌入；特别地，在 $\mathbb{Q}$ 上的每个阿贝尔簇，只要在 $\mathbb{Q}$ 上同源于椭圆曲线的乘积；(b) $A = \mathrm{Res}_{F/K}E$ 是有限扩张F/K上的椭圆曲线 E 的魏尔限制，其中 E 具有复乘，或者 $\mathbb{Q}(j(E))$ 具有实嵌入。

如果 $K = \mathbb{Q}$, F 是二次的，并且 E 在 F 上不同源于 $\mathbb{Q}$上某条椭圆曲线的基变换，那么 ***(b)*** 中的$\mathrm{Res}_{F/\mathbb{Q}}E$ 是 $\mathbb{Q}$上的简单阿贝尔曲面。

证明。 **(a)** 每个 E_i 根据命题 11.1都有一个超奇异素数；取 $K' = K$.

(b) 设 K' 是 F/K的伽罗瓦闭包。在 K'上，$\mathrm{Res}_{F/K}E$ 同构于 $\prod_\sigma E^\sigma$，即关于 K-嵌入 σ 的乘积： $F \to K'$ [15, §1]。如果E 具有复乘，则每个 E^σ 也具有复乘；而 $\mathbb{Q}(j(E^\sigma)) = \sigma(\mathbb{Q}(j(E)))$ 同构于 $\mathbb{Q}(j(E))$，因此如果 $\mathbb{Q}(j(E))$具有实嵌入，则它也具有实嵌入。根据命题 **11.1**，每个 E^σ 都有一个超奇异素数，定理 **C** 适用。

对于最后一个断言， $A = \mathrm{Res}_{F/\mathbb{Q}}E$ 是一个阿贝尔曲面。若它在 $\mathbb{Q}$上不是单的，则它在 $\mathbb{Q}$ 上同源于 $E_1 \times E_2$，其中 E_i 是定义在 $\mathbb{Q}$上的椭圆曲线。在 F上， $A_F \cong E \times E^\sigma$，其中 σ 是 F的非平凡自同构，因此 $E \times E^\sigma$ 在 F 上同源于$(E_1)_F \times (E_2)_F$；根据庞加莱完全可约定理，E在 F上同源于$(E_1)_F$ 或$(E_2)_F$。 □

References

[1] M. Baker，动力学格林函数平均值的下界， *Math. Res. Lett.* 13 （2006），245–257。[2] M. Baker 和 C. Petsche，椭圆曲线上的整体差异与小点， *Int. Math. Res. Not.* 2005，第 61 号，3791–3834。[3] E. Bombieri 和 U. Zannier，关于某些 $\mathbb{Q}$ 的无限扩张中的高度的注记， *Rend. Mat. Acc. Lincei*（9）12（2001），5–14。[4] G. S. Call 和 J. H. Silverman，带态射的簇上的典范高度， *Compositio Math.* 89 （1993），163–205。[5] J. Cheon 和 S. Hahn，椭圆曲线除法多项式的显式赋值， *Manuscripta Math.*97（1998），319–328。[6] N. D. Elkies，每条定义在 $\mathbb{Q}$ 上的椭圆曲线都有无穷多个超奇异素数， *Invent.Math.* 89（1987），561–567。[7] N. D. Elkies，实数域上的椭圆曲线的超奇异素数， *Compositio Math.* 72（1989），165–172。[8] ´E. Gaudron 和 G. R´emond，阿贝尔簇上的小点计数，´et´é ab´elienne， *J. Inst. Math. Jussieu* 24（2025），705–761。[9] M. Hindry 和 J. H. Silverman，关于椭圆曲线的 Lehmer 猜想，载于 *Séminaire de Théorie des Nombres, Paris 1988–1989*，Progr. Math. 91，Birkh¨auser，1990，103–116。[10] M. Hindry 和 J. H. Silverman， *Diophantine Geometry: An Introduction*，GTM 201，Springer，2000。

[11] S. Lang, *Elliptic Functions*，第 2 版，GTM 112，Springer，1987。[12] M. Laurent，N´eron–Tate 高度的下界，载于 *Séminaire de Théorie des Nombres, Paris 1981–82*，Progr. Math. 38，Birkh¨auser，1983，137–151。[13] D. W. Masser，椭圆曲线上小高度点的计数， *Bull. Soc. Math. France* 117 （1989），247–265。[14] D. W. Masser 致 D. Bertrand 的信，1986年11月17日。[15] J. S. Milne，关于阿贝尔簇的算术， *Invent. Math.* 17（1972），177–190。[16] J. H. Silverman, *The Arithmetic of Elliptic Curves*，第 2 版，GTM 106，Springer，2009。