

超奇异素数和博戈莫洛夫性质

Soumyadip Sahu

School of Mathematics, Tata Institute of Fundamental Research
1 Homi Bhabha Road, Mumbai, 400005, Maharashtra, India.

Email: soumyadip.sahu00@gmail.com

Abstract

令 E 是在数域 K 上的一个椭圆曲线，该数域至少有一个实嵌入，并且 L 是 K 的一个有限扩张。我们将 Habegger 的结果推广到表明 $L(E_{\text{tor}})$ ，即由 E 在 L 上的挠点生成的域，具有 Bogomolov 性质。此外， $E(L(E_{\text{tor}}))$ 上的 Néron-Tate 高度也满足类似的离散性质。我们的主要工具是 Plessis 的一个一般准则，该准则将问题归结为存在满足某些条件的 E 的超奇异素数。

MSC2020: 主要 11G50，次要 11G05

关键词: 博戈莫洛夫性质，超奇异素数

1 结果声明

代数数的绝对对数 Weil 高度（简写为高度）是一个非负实数 [5]，用于衡量其算术复杂性。根据 Northcott 定理，有界次数和有界高度的代数数只有有限多个。Kronecker 定理告诉我们，一个代数数的高度为零当且仅当它是零或单位根。因此，对于给定的一个数域，存在 $\epsilon > 0$ 使得该域中每个元素（除了零和单位根之外）的高度都大于 ϵ 。这一现象启发了以下定义。我们说一个代数扩张 $L/\mathbb{Q}$ 具有博戈莫洛夫性质，如果存在 $\epsilon > 0$ 使得 $L^\times$ 中每个高度为 $< \epsilon$ 的元素都是单位根。这个性质的名称来源于 Bogomolov 关于

代数曲线上的小高度点的一个类似猜想，这些代数曲线的亏格是 ≥ 2 。近年来，许多数论学家研究了从算术和几何来源产生的各种无限代数扩张类的 Bogomolov 性质 [1]。例如，Amoroso 和 Zannier 在 Amoroso 和 Dvornicich 的早期工作基础上，[3]，表明数域 K 的最大阿贝尔扩张 K^{ab} 具有 Bogomolov 性质。还可以通过将 Weil 高度替换为 Néron-Tate 高度来推广 Bogomolov 性质到椭圆曲线的概念。更详细地说，设 E 是一个定义在数域 K 上的椭圆曲线。给定一个代数扩张 L/K ，我们说群 $E(L)$ 具有博戈莫洛夫性质如果存在 $\epsilon > 0$ 使得 $E(L)$ 上每个具有 Néron-Tate 高度 $< \epsilon$ 的点都是挠点。几位作者研究了椭圆 Bogomolov 性质，以说明环面和椭圆曲线算术之间的相似性。例如，Silverman[14] 表明如果 E 是数域 K 上的椭圆曲线，则 $E(K^{\text{ab}})$ 具有 Bogomolov 性质。我们感兴趣的是 Habegger[9] 的一个显著结果，该结果证明了由椭圆曲线的挠点生成的域具有 toric 和 elliptic Bogomolov 性质。

我们固定一个代数闭包 $\overline{\mathbb{Q}}$ 为 $\mathbb{Q}$ 并且处理 $\overline{\mathbb{Q}}$ 的子域。设 μ_∞ 是 $\overline{\mathbb{Q}}$ 中的单位根集合。对于数域 K 上的椭圆曲线 E ，令 E_{tor} 表示 $E(\overline{\mathbb{Q}})$ 的挠子群。现在假设 L/K 是一个代数扩张。那么 $L(E_{\text{tor}})$ 是由 E 的扭转点的坐标在 L 上生成的域，对于 K -有理魏尔斯特拉斯模型而言。这个域不依赖于魏尔斯特拉斯模型的选择。

定理 1.1. (哈贝格) 设 E 是在 $\mathbb{Q}$ 上定义的椭圆曲线。那么 $\mathbb{Q}(E_{\text{tor}})$ 具有博戈莫洛夫性质。此外，群 $E(\mathbb{Q}(E_{\text{tor}}))$ 具有椭圆博戈莫洛夫性质。

Amoroso 和 Terracini[2] 探讨了为与兼容的 ℓ -adic Galois 表示关联的无限扩张来表述定理 1.1 的可能性。

特别是，可以询问 Habegger 结果的以下推广是否成立：

Conjecture. 令 E 是数域 K 上的椭圆曲线。则 $K(E_{\text{tor}})$ 和 $E(K(E_{\text{tor}}))$ 具有博戈莫洛夫性质。

请注意，如果 L/K 是有限扩张，那么可以将 E 视为定义在 L 上的椭圆曲线，从而从该猜想中得出关于 $L(E_{\text{tor}})$ 的陈述。因此，上述猜想等价于以下更强的版本：

猜想 1.2. 设 E 是数域 K 上的椭圆曲线，且 L/K 是有限扩张。则 $L(E_{\text{tor}})$

和 $E(L(E_{\text{tor}}))$ 具有博戈莫洛夫性质。

如果 L 是一个具有 Bogomolov 性质的代数扩张，并且 F/L 是一个有限扩张，那么 F 不必具备 Bogomolov 性质；参见 [1]。对于一个具有复乘法的椭圆曲线，猜想 1.2 是 Amoroso-Zannier 和 Silverman 关于极大阿贝尔扩张的结果（命题 2.2）的一个简单推论。Habegger 工作的重点是通过仔细运用伽罗瓦理论和平均分布定理来处理非 CM 的情况。在后续的发展中，Frey[8] 将 Habegger 的论证推广到建立关于椭圆曲线上 Conjecture 1.2 的域扩张部分，对于 $\mathbb{Q}$ 。她的工作还提供了一个关于 Weil 高度的明确下界，以椭圆曲线的一个合适的超奇异素数为条件。最近，Plessis[10] 改进了 Frey 的工作，推导出一个非常一般的准则，用于由数域上椭圆曲线的挠点生成的域的 Bogomolov 性质，在我们的工作中起着关键作用。

设 L/K 是数域的有限扩张。给定 K 的一个有限点 v ，我们记 $e_w(L|K)$ ，相应地记 $f_w(L|K)$ ，为分歧指数，相应地。剩余度，地点 w 的 L 与 $w|v$ 。此外，设

$$d_v(L) = \max_{w|v} [L_w : K_v].$$

我们用 $h(\cdot)$ 表示一个代数数的魏尔高度。

定理 1.3. (普莱西) 令 E 是在一个数域 K 上定义的椭圆曲线。假设 L/K 是一个有限伽罗瓦扩张。现在假设 v 是一个位于有理素数 p 上的 K 的地方，使得

(i) E 在 v 和 $j_E \not\equiv 0, 1728 \pmod{v}$ 处有超奇异约化，

(ii) $p > \max\{3, 2d_v(L)\}$ 以及规范 $Galois$ 表示的像

$$(1.1) \quad \text{Gal}(L(E[p])/L) \rightarrow \text{GL}_2(\mathbb{Z}/p\mathbb{Z})$$

包含 $\text{SL}_2(\mathbb{Z}/p\mathbb{Z})$,

(iii) $e_v(K|\mathbb{Q}) = 1$ 和 $f_v(K|\mathbb{Q}) \leq 2$ 。

然后，对于所有的 $\alpha \in L(E_{\text{tor}})^\times \setminus \mu_\infty$ ，我们有

$$h(\alpha) \geq \frac{1}{4p^{2d_v(L)} + 1} \left(\frac{\log p}{d_v(L)(40\sqrt{2} + 2)[K:\mathbb{Q}]p^{2p^{2d_v(L)}+2}} \right)^{2 + \frac{4}{p^{p^{2d_v(L)}/4} - 2}}.$$

此外, 如果

(iv) v 在 L 中是无分歧的,

(v) (ii) 中的表示是满射的,

那么 $E(L(E_{\text{tor}}))$ 具有 *Bogomolov* 性质。

直接应用这个定理的一个明显障碍是找到一个满足条件的超奇异素数。然而, Elkies[7] 证明了如果基域 K 至少有一个实嵌入, 则 E 在 K 的无穷多素数处是超奇异的。Plessis 利用这一结果将定理 1.1 推广到实二次域上的椭圆曲线。本短文的目的是证明, 如果我们研究定义在最小定义域上的椭圆曲线问题, 即 $\mathbb{Q}(j_E)$, 其中 j_E 是 E 的 j -不变量, 则定理 1.3 中的第三个条件根本不会造成任何困难。因此, 可以结合 Serre 和 Plessis 的结果, 得到猜想 1.2 的一个特殊情况。该结果的一个版本先前在作者的硕士学位论文 [11] 中已宣布并证明了附加假设。

定理 1.4. 设 E 是数域 K 上的一个椭圆曲线, 使得 E 有无限多个超奇异素数。那么猜想 1.2 对 E 成立。

我们也提供了当定理成立时, 关于 $L(E_{\text{tor}})$ 的高度的一个显式下界 (命题 2.4)。可以利用 Elkies 的无穷性结果直接从上述定理推导出一大类椭圆曲线的猜想。

推论 1.5. 令 E 是数域 K 上的椭圆曲线。假设 $\mathbb{Q}(j_E)$ 至少有一个实嵌入。则椭圆曲线 E 满足猜想 1.2。特别地, 如果 K 本身至少有一个实嵌入, 则猜想 1.2 对 E 成立。

关于在完全虚数域上的椭圆曲线的超奇异素数的存在性, 没有普遍的结果。

例如, Elkies[6] 考虑了椭圆曲线

$$E : iy^2 = x^3 + (i - 2)x^2 + x \text{ over } K = \mathbb{Q}(i) \text{ with } j_E = \frac{2^{14}}{i - 4},$$

并使用计算机验证了 E 没有位于小于 74000 的奇素数上的超奇异素数。然而, 他提供了一个启发式的论证, 推测 E 在某个 $C > 0$ 下应该有 $C \log \log x$

个超奇异素数, 直到 x 为 $x \rightarrow \infty$ 。如果这个猜想是正确的, 那么定理 1.4 将意味着上述描述的曲线 E 上的猜想 1.2。

2 论证的细节

令 E 是数域 K 上具有 j -不变量 j_E 的椭圆曲线。我们知道 E 在 $\mathbb{Q}(j_E)$ 上有一个模型, 且任何具有此性质的域都包含 $\mathbb{Q}(j_E)$ [13, p.45]。为了方便起见, 记 $K_E := \mathbb{Q}(j_E)$, 并令 $\mathcal{O}_{K_E}$ 表示 K_E 的整环。我们的主要观点如下:

引理 2.1. 令 E 是在 K_E 上定义的椭圆曲线。然后, 存在一个有限子集 S , 它是 $\mathcal{O}_{K_E}$ 的素理想集合, 包含了在扩张 $K_E/\mathbb{Q}$ 中分歧的素数, 使得每个位于 S 之外的超奇异素数相对于 $\mathbb{Q}$ 的剩余度为 1 或 2。

Proof. 写出 $j_E \mathcal{O}_{K_E} = \mathfrak{a} \mathfrak{b}^{-1}$, 其中 $\mathfrak{a}$ 和 $\mathfrak{b}$ 是非零互质整理想。令 $N = |\mathcal{O}_{K_E}/\mathfrak{b}|$ 。那么 $\mathfrak{b} \mid N \mathcal{O}_{K_E}$ 和 $N j_E \in \mathcal{O}_{K_E}$ 。观察到由 $N j_E$ 生成的子环 $\mathbb{Z}[N j_E]$ 是 K_E 内的一个阶, 即 $\mathbb{Z}[N j_E]$ 是 $\mathcal{O}_{K_E}$ 的一个有限指数 $\mathbb{Z}$ -子模。定义 S 为由除理性整数

$$N D_{K_E}[\mathcal{O}_{K_E} : \mathbb{Z}[N j_E]]$$

的素理想组成的 $\mathcal{O}_{K_E}$ 的场所集合, 其中 D_{K_E} 是 $K_E/\mathbb{Q}$ 的判别式, $[\mathcal{O}_{K_E} : \mathbb{Z}[N j_E]]$ 是子格 $\mathbb{Z}[N j_E]$ 在 $\mathcal{O}_{K_E}$ 中的指数。现在假设 $\mathfrak{p} \notin S$ 和 p 是位于 $\mathfrak{p}$ 下方的有理素数。根据构造, p 与 $[\mathcal{O}_{K_E} : \mathbb{Z}[N j_E]]$ 互质。因此可以将 $- \otimes_{\mathbb{Z}} \mathbb{Z}/p\mathbb{Z}$ 应用于包含关系 $\mathbb{Z}[N j_E] \rightarrow \mathcal{O}_{K_E}$, 以发现

$$\mathcal{O}_{K_E}/p\mathcal{O}_{K_E} = \mathbb{Z}/p\mathbb{Z}[\overline{N j_E}].$$

这里 $\overline{N j_E}$ 是 $N j_E$ 在 $\mathcal{O}_{K_E} \twoheadrightarrow \mathcal{O}_{K_E}/p\mathcal{O}_{K_E}$ 下的像, 而 $\mathbb{Z}/p\mathbb{Z}[\overline{N j_E}]$ 是由 $\overline{N j_E}$ 生成的 $\mathbb{Z}/p\mathbb{Z}$ -子代数。由于 p 在 K_E 中不分歧, 我们有 $p\mathcal{O}_{K_E} = \prod_{\mathfrak{p}|p} \mathfrak{p}$, 其中乘积遍历 $\mathcal{O}_{K_E}$ 中的素数。因此, $\mathcal{O}_{K_E}/p\mathcal{O}_{K_E} \cong \prod_{\mathfrak{p}|p} \mathcal{O}_{K_E}/\mathfrak{p}$ 作为 $\mathbb{Z}/p\mathbb{Z}$ -代数。投影到对应于 $\mathfrak{p}$ 的因素上, 我们看到

$$\mathcal{O}_{K_E}/\mathfrak{p} = \mathbb{Z}/p\mathbb{Z}[\widetilde{N j_E}]$$

其中 $\widetilde{N j_E}$ 指的是在约简 $\mathcal{O}_{K_E} \twoheadrightarrow \mathcal{O}_{K_E}/\mathfrak{p}$ 下的像, 并且 $\mathbb{Z}/p\mathbb{Z}[\widetilde{N j_E}]$ 是由 $\widetilde{N j_E}$ 生成的 $\mathbb{Z}/p\mathbb{Z}$ -子代数。再次选择 $\mathfrak{p}$ 确保 j_E 在 $\mathfrak{p}$ 处是整数。令 $\mathcal{O}_{K_E, \mathfrak{p}}$ 为 $\mathcal{O}_{K_E}$

在 $\mathfrak{p}$ 处的局部化, 且 $\widetilde{j_E}$ 为 j_E 在 $\mathcal{O}_{K_E, \mathfrak{p}} \rightarrow \mathcal{O}_{K_E}/\mathfrak{p}$ 下的像。由于 $p \nmid N$, 显然有 $\mathbb{Z}/p\mathbb{Z}[\widetilde{Nj_E}] = \mathbb{Z}/p\mathbb{Z}[\widetilde{j_E}]$ 。现在假设 $\mathfrak{p}$ 是椭圆曲线 E 的超奇异简约素数。然后 E 在 $\mathfrak{p}$ 处有良好约化, 并且 $\widetilde{j_E}$ 等于约化的椭圆曲线的 j 不变量。因此 $\widetilde{j_E}$ 位于 $\mathbb{Z}/p\mathbb{Z}$ 的二次扩张中 (定理 3.1 在 [13, V.3] 中)。但 $\mathcal{O}_{K_E}/\mathfrak{p} = \mathbb{Z}/p\mathbb{Z}[\widetilde{j_E}]$ 。因此扩展 $\mathcal{O}_{K_E}/\mathfrak{p}$ 在 $\mathbb{Z}/p\mathbb{Z}$ 上的次数必须是 ≤ 2 。由此可知, 任何超奇异素数 $\mathfrak{p}$ 属于 E 且不在我们的集合 S 之外的都满足 $f_{\mathfrak{p}}(K_E|\mathbb{Q}) \leq 2$ 如所期望的那样。 $\square$

引理 2.1 允许我们将 Plessis 的判据应用于具有无限多个超奇异素数的椭圆曲线, 前提是伽罗瓦表示 (1.1) 在一个大的超奇异素数处具有大像。因此, 由于阿贝尔行为导致后者条件失败, 方便将 CM 情况单独处理。

命题 2.2. 设 E 是在数域 K 上定义的具有复乘法的椭圆曲线, L/K 是一个有限扩张。然后猜想 1.2 成立 E 。此外, 对于每个 $\alpha \in L(E_{\text{tor}})^{\times} \setminus \mu_{\infty}$, 我们有

$$h(\alpha) > 3^{-4d^2-4d-6}$$

其中 $d = [L : \mathbb{Q}]$ 。

Proof. 假设 E 由某个正整数 D 的 $\mathbb{Q}(\sqrt{-D})$ 中的一个阶进行复乘。设 $K_D = K(\sqrt{-D})$ 和 $L_D = L(\sqrt{-D})$ 。然后, 复乘理论断言 $K_D(E_{\text{tor}}) \subseteq K_D^{\text{ab}}$ 。特别是, $L(E_{\text{tor}}) \subseteq L_D(E_{\text{tor}}) \subseteq L_D^{\text{ab}}$ 。因此, 应用 Amoroso-Zannier 的结果 [3] 和 Silverman 的结果 [14] (在第 1 节中陈述), 表明 $L(E_{\text{tor}})$ 和 $E(L(E_{\text{tor}}))$ 具有 Bogomolov 性质。对于 Weil 高度的显式下界, 我们需要对上述使用的结果进行定量细化。令 F 是一个次数为 n 的数域, 并且令 $\alpha \in \overline{\mathbb{Q}}^{\times} \setminus \mu_{\infty}$ 是一个代数数, 使得 $F(\alpha)/F$ 是阿贝尔的。Amoroso 和 Zannier 在后续论文 [4] 中得到了以下显式界:

$$(2.1) \quad h(\alpha) > 3^{-n^2-2n-6}.$$

我们取 $F = L_D$ 。因此 $n = [L_D : \mathbb{Q}] \leq 2d$ 和陈述中的不等式是 (2.1) 的结果。 $\square$

在证明定理 1.4 之前, 我们提出一个简单的观察以澄清该定理的假设。

引理 2.3. 令 E 是数域 K 上的椭圆曲线, 并且 L/K 是有限扩张。那么, E/K 有无限多个超奇异素数当且仅当 E/L 也有无限多个超奇异素数。

Proof. 对于有限域上的椭圆曲线, 超奇异性 [13, p.145] 的定义仅涉及其在代数闭包上的性质。因此, 如果 E/K 在 K 的素数 $\mathfrak{p}$ 处具有超奇异约化, 则 E/L 在满足 $\mathfrak{P} \mid \mathfrak{p}$ 的 L 的每个素数 $\mathfrak{P}$ 处也具有超奇异约化。请注意, 在这种情况下, E/L 自动在每个 $\mathfrak{P}$ [13, p.197] 处具有良好的约化。反之, 若 E/L 在 L 的素理想 $\mathfrak{P}$ 处为超奇异, 则当 E 在 $\mathfrak{p}$ 处有良约化时, E/K 在 $\mathfrak{p} = \mathfrak{P} \cap K$ 处亦呈超奇异。由于任意椭圆曲线仅有有限多个坏约化素理想, 该引理由此两观测结果得出。 $\square$

定理 1.4 的证明。 令符号与定理陈述中的相同。我们在命题 2.2 中已经处理了 CM 情形。假设 E 没有复乘。如前所述, 写作 $K_E = \mathbb{Q}(j_E)$, 并设 E_0 为域 K_E 上的 E 的模型。为了具体起见, 固定一个定义在有限扩张 K'/K 上的同构 $\varphi : E_0 \xrightarrow{\cong} E$ 。根据引理 2.3, 该定理的假设确保了 E/K' 有无限多个超奇异素数。因此, 可以使用同构 φ 和引理 2.3 中的下降语句来得出结论: E_0/K_E 也有无限多个超奇异约化素数。此外, 由引理 2.1 可知, 除了有限多个超奇异素数外, E_0/K_E 的所有超奇异素数的剩余度为 1 或 2。定义 L' 为 $K'L$ 在 K_E 上的伽罗瓦闭包。我们希望将 Plessis 的判据应用于配对 $(E_0/K_E, L'/K_E)$ 。由于 E_0 没有复乘, Serre 的一个著名定理 [12] 表明, 对于除了有限多个有理素数 p 之外的所有情况, 伽罗瓦表示 (1.1) 是满射的。此外, 参数 $d_v(L')$ 统一上界于扩张的程度 L'/K_E 。因此, 存在一个大的超奇异素数 v , 使得定理 1.3 中的 (i)-(v) 对于成对出现的 $(E_0/K_E, L'/K_E)$ 成立。作为结果, $L'(E_{0,\text{tor}})$ 和 $E_0(L'(E_{0,\text{tor}}))$ 具有 Bogomolov 性质。为了完成定理的证明, 只需验证 $L'(E_{\text{tor}})$ 和 $E(L'(E_{\text{tor}}))$ 具有 Bogomolov 性质。第一部分是显而易见的, 因为同构 φ 诱导了一个等式 $L'(E_{0,\text{tor}}) = L'(E_{\text{tor}})$ 。最后, Néron-Tate 高度的唯一性 (定理 9.3 在 [13, VIII.9] 中) 表明通过 φ 将 $E(\overline{\mathbb{Q}})$ 上的 Néron-Tate 高度拉回到 $E_0(\overline{\mathbb{Q}})$ 等于 $E_0(\overline{\mathbb{Q}})$ 上的 Néron-Tate 高度。 $E(L'(E_{\text{tor}}))$ 在 φ 下的原像正是 $E_0(L'(E_{\text{tor}}))$ 。因此, $E(L'(E_{\text{tor}}))$ 也具有博戈莫洛夫性质。 $\square$

推论 1.5 的证明。 令 E 是数域 K 上的一个椭圆曲线, 使得 $K_E = \mathbb{Q}(j_E)$ 至少有一个实嵌入。与之前一样, 只需处理 E 没有复乘的情形。回忆定理 1.4 的证明中所用到的符号 E_0 , φ 和 K' 。由于 K_E 有一个实嵌入, 根据 Elkies 定理 [7] 我们知道 E_0/K_E 有无限多个超奇异素数。现在, 可以使用同构 φ 和引理 2.3 来推导出 E/K' , 因此 E/K 有无限多个超奇异素数。因此, 这一断言是定理 1.4 的结果。

也可以根据一些相关参数写出 Weil 高度的一个明确下界。

命题 2.4. 令符号如定理 1.4 中所示, 并假设 E 没有复乘。令 v 为 K_E 的一个位置, 使得在定理 1.4 的证明中描述的对关系 $(E_0/K_E, L'/K_E)$ 满足定理 1.3 中的 (i)-(iii)。那么, 对于每一个 $\alpha \in L(E_{\text{tor}})^\times \setminus \mu_\infty$, 我们有

$$h(\alpha) \geq \frac{1}{4p^{2d_v(L')} + 1} \left(\frac{\log p}{d_v(L')(40\sqrt{2} + 2)[K_E : \mathbb{Q}]p^{2p^{2d_v(L')} + 2}} \right)^{2 + \frac{4}{p^{2d_v(L')/4 - 2}}}.$$

证明定理 1.4 中给出的论据表明, 存在无穷多个地点 v 满足命题的假设。

Proof. 由定理 1.3 应用于配对 $(E_0/K_E, L'/K_E)$ 得出。 $\square$

Néron-Tate 高度的显式下界似乎更难获得, 这是因为椭圆等分布结果的有效性不足; 参见 [10] 中的备注 1.7。

致谢

我要感谢一位匿名评审人仔细阅读了手稿并就其呈现提出了诸多改进意见。

References

- [1] F.Amoroso, S.David, U.Zannier; *On fields with property (B)*, Proc. Amer. Math. Soc., **142**(6), pp. 1893-1910 (2014) <https://www.jstor.org/stable/23809602>
- [2] F. Amoroso, L.Terracini; *Bogomolov property and Galois representations*, Arxiv preprint (2024) <https://doi.org/10.48550/arXiv.2403.03319>

- [3] F. Amoroso, U. Zannier; *A relative Dobrowolski lower bound over abelian extensions*, Ann. Sc. Norm. Super. Pisa Cl. Sci. (4), **29**(3), pp. 711-727 (2000) http://www.numdam.org/item/ASNSP_2000_4_29_3_711_0/
- [4] F. Amoroso, U. Zannier; *A uniform relative Dobrowolski lower bound over abelian extensions*, Bull. Lond. Math. Soc., **42**(3), pp. 489-498 (2010) <https://doi.org/10.1112/blms/bdq008>
- [5] E.Bombeiri, W.Gubler; *Heights in Diophantine geometry*, New mathematical monographs, Vol 4, Cambridge University Press, Cambridge (2006)
- [6] N.D.Elkies; *The existence of infinitely many supersingular primes for every elliptic curve over $\mathbb{Q}$* , Invent. Math., **89**, pp. 561-567 (1987) <https://doi.org/10.1007/BF01388985>
- [7] N.D.Elkies; *Supersingular primes for elliptic curves over real number fields*, Compos. Math., **72**(2), pp. 165-172 (1989) http://www.numdam.org/item?id=CM_1989__72_2_165_0
- [8] L.Frey; *Small heights in large non-Abelian extensions*, Ann. Sc. Norm. Super. Pisa Cl. Sci. (5), **23**(3), pp. 1357-1393 (2022) https://doi.org/10.2422/2036-2145.201811_018
- [9] P.Habegger; *Small height and infinite nonabelian extensions*, Duke Math. J., **162**(11), pp. 2027-2076 (2013) <http://doi.org/10.1215/00127094-2331342>
- [10] A.Plessis; *Bogomolov property of some infinite nonabelian extensions of a totally v -adic field*, Acta Arith., **213**, pp. 1-23 (2024) <https://doi.org/10.4064/aa220216-31-1>
- [11] S.Sahu; *Points of small height in certain nonabelian extensions*, Master's thesis, Chennai Mathematical Institute (2018) Available at: <https://>

[//doi.org/10.48550/arXiv.1806.06587](https://doi.org/10.48550/arXiv.1806.06587)

- [12] J.P.Serre; *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*, Invent. Math., **15**, pp. 259-331 (1971) <https://doi.org/10.1007/BF01405086>
- [13] J.H.Silverman; *The arithmetic of elliptic curves*, Graduate texts in mathematics, Vol 106, Second edition, Corrected second print, Springer, New York (2009)
- [14] J.H.Silverman; *A lower bound for the canonical height on elliptic curves over abelian extensions*, J. Number Theory, **104**(2), pp. 353-372 (2004) <https://doi.org/10.1016/j.jnt.2003.07.001>