中国科学: 数学 2024 年 第 54 卷 第 9 期: 1283 ~ 1296
SCIENTIA SINICA Mathematica
论 文

《中国科学》杂志社
SCIENCE CHINA PRESS
CrossMark click for updates

有理数域上带复乘椭圆曲线的 Birch-Swinnerton-Dyer 猜想

献给陆洪文教授 85 寿辰

李永雄[1], 刘余[1], 田野[2,3,4*]

1. 清华大学丘成桐数学科学中心, 北京 100084;
2. 中国科学院大学数学科学学院, 北京 100049;
3. 中国科学院数学与系统科学研究院, 北京 100190;
4. 中国科学院晨兴数学中心, 北京 100190
E-mail: yongxiongli@gmail.com, yliu2018@mail.tsinghua.edu.cn, ytian@math.ac.cn

收稿日期: 2023-12-28; 接受日期: 2024-04-26; 网络出版日期: 2024-06-04; * 通信作者
国家自然科学基金 (批准号: 12288201 和 11531008) 资助项目

摘要 设 E 是 $\mathbb{Q}$ 上带复乘 K 的椭圆曲线, p 是一个奇素数使得 E 在 p 处有潜在好通常约化. 本文证明, 若 $L(s,E)$ 在 $s=1$ 处有单零点, 则 E 的 p- 部分 Birch-Swinnerton-Dyer 猜想成立. 进一步地, 本文给出一族椭圆曲线, 其导子可以被任意数目的素数整除, 具有秩 1 且满足完整的 Birch-Swinnerton-Dyer 猜想.

关键词 Birch-Swinnerton-Dyer 猜想 复乘理论 椭圆曲线

MSC (2020) 主题分类 11G40

1 引言

设 E 是定义在数域 F 上的椭圆曲线. 设 $L(s,E/F)$ 是 E 在 F 上的复 L- 函数, $E(F)$ (相应地, $Ш(E/F)$) 是 E 在 F 上的 Mordell-Weil 群 (相应地, Shafarevich-Tate 群). 对于任意素数 p, 用 $Ш(E/F)[p^\infty]$ 表示 $Ш(E/F)$ 的 p- 准素部分. 当 $F=\mathbb{Q}$ 时, 简记 $L(s,E)=L(s,E/\mathbb{Q})$. 由 Wiles [17] 证明的模性定理可知 $L(s,E)$ 是 $\mathbb{C}$ 上的全纯函数 (也可参见文献 [2]).

设 v 是 F 的一个素位, 令 F_v 为 F 在 v 处的完备域. 如果存在 F_v 的一个有限域扩张 L, 使得 E 在 L 上具有好通常约化, 则称 E 在 v 处有潜在好通常约化.

定理 1.1 令 E 是有理数域 $\mathbb{Q}$ 上带复乘的椭圆曲线, p 是奇素数, 且 E 在 p 处有潜在好通常约化.

英文引用格式: Li Y X, Liu Y, Tian Y. The Birch-Swinnerton-Dyer conjecture of elliptic curves over $\mathbb{Q}$ with complex multiplication (in Chinese). Sci Sin Math, 2024, 54: 1283–1296, doi: 10.1360/SSM-2023-0342

© 2024《中国科学》杂志社

(i) 如果 $L(s,E)$ 在 $s=1$ 处有单零点, 则 $E(\mathbb{Q})$ 的秩是 1 且 $Ш(E/\mathbb{Q})$ 是有限群. 进一步地, $Ш(E/\mathbb{Q})[p^\infty]$ 的阶与 Birch-Swinnerton-Dyer 猜想的猜测值吻合.

(ii) 如果 $E(\mathbb{Q})$ 的秩是 1 且 $Ш(E/\mathbb{Q})[p^\infty]$ 有限, 则 $L(s,E)$ 在 $s=1$ 处有单零点.

注 1.1 定理 1.1(i) 的第一部分是 Gross-Zagier 和 Kolyvagin 的结果; 剩下的部分, 因为 Rubin 证明了虚二次域的 Iwasawa 主猜想, 对好通常约化的素数, 这是 Perrin-Riou 的结果 [12]. 本文处理的是一般有潜在好通常约化的素数. 这个结果可以很容易地推广到 $\mathbb{Q}$ 上带复乘中心特征平凡的权为 2 的模形式给出的 Abel 簇.

下面的定理证明了, 在有理数域 $\mathbb{Q}$ 上, 存在无穷多条椭圆曲线, 其导子可被任意数目的素数整除, 它们的秩为 1 且满足完整的 Birch-Swinnerton-Dyer 猜想, 即相应的 Birch-Swinnerton-Dyer 猜想的秩部分和精细部分都成立.

定理 1.2 令 $n\equiv 5 \pmod 8$ 是没有平方因子的正整数, 并且其素因子都模 4 同余于 1. 假设 $\mathbb{Q}(\sqrt{-n})$ 的类群没有 4 阶元, 对于有理数域上的椭圆曲线 $E^{(n)}: y^2=x^3-n^2x$, 它的秩为 1 且满足完整的 Birch-Swinnerton-Dyer 猜想. 特别地, 对于任意模 8 同余于 5 的素数 p, 椭圆曲线 $E^{(p)}$ 的秩为 1 且完整的 Birch-Swinnerton-Dyer 猜想成立.

证明 用类似于文献 [15] (或文献 [16]) 中的归纳法, 可以证明定理 1.3 中的用 Gross-Prasad 测试向量构造的 Heegner 点 P 不是挠点, 则

$$E^{(n)}: y^2=x^3-n^2x$$

的解析秩和代数秩都是 1.

注意到 $E^{(n)}$ 的精细 Birch-Swinnerton-Dyer 猜想是关于两个有理数的等式, 对于素数 ℓ, 如果这两个有理数在 ℓ 处具有相同的阶, 则称 ℓ- 部分 Birch-Swinnerton-Dyer 猜想成立.

由 Perrin-Riou [12] 和 Kobayashi [10] 的结果知, 对于任意与 n 互素的奇素数 p, $E^{(n)}$ 的 p- 部分 Birch-Swinnerton-Dyer 猜想成立. 记 $\mathrm{Sel}_2(E^{(n)}/\mathbb{Q})$ 是 $E^{(n)}$ 的 2-Selmer 群, $E^{(n)}(Q)_{\mathrm{tor}}$ 是 $E^{(n)}(\mathbb{Q})$ 的挠点构成的群. 在定理关于 $\mathbb{Q}(\sqrt{-n})$ 的类群假设下, 利用 2- 下降, 可知

$$\dim_{\mathbb{F}_2}\mathrm{Sel}_2(E^{(n)}/\mathbb{Q})/\mathrm{Im}(E^{(n)}(\mathbb{Q})_{\mathrm{tor}})=1. \tag{1.1}$$

根据精确版本的 Gross-Zagier 公式 (参见文献 [4]), $E^{(n)}$ 的 2- 部分 Birch-Swinnerton-Dyer 猜想恰好是下面定理 1.3 中证明的关于点 P 的 2- 可除性. 最后, 对于整除 n 的素数 p, 注意到 $p\equiv 1 \pmod 4$, 故 $E^{(n)}$ 在 p 处有潜在好通常约化, 由定理 1.1, 从而 $E^{(n)}$ 的 p- 部分 Birch-Swinnerton-Dyer 猜想成立. □

为了在 $\mathbb{Q}$ 上求解 Diophantine 方程

$$y^2=x^3-n^2x,$$

考虑下述复合映射定义的 $E^{(n)}$ 的复参数化:

$$\mathcal{H}\xrightarrow{\pi}\Gamma_0(32)\backslash\mathcal{H}\cup P^1(\mathbb{Q})=X_0(32)\xrightarrow{f_0}E^{(1)}\xrightarrow{[2-2i]}E^{(1)}\xrightarrow{\iota}E^{(n)},$$

其中,

- $\mathcal{H}\xrightarrow{\pi}\Gamma_0(32)\backslash(\mathcal{H}\cup P^1(\mathbb{Q}))=X_0(32)(\mathbb{C})$ 是通常的商映射;
- $f_0: X_0(32)\to E^{(1)}$ 是定义在 $\mathbb{Q}$ 上将 $[\infty]$ 映为 O 的、次数为 2 的映射;

• $[2-2\mathrm{i}]$ 是 $E^{(1)}$ 上由 $2-2\mathrm{i}$ 给出的复乘, 其中 $\mathrm{i}(x,y)=(-x,\mathrm{i}y)$;

• $\iota: E^{(1)}\xrightarrow{\sim} E^{(n)}$ 是扰动映射: $(x,y)\mapsto(-nx,(-n)^{3/2}y)$.

正如定理 1.2 的证明中指出的, 下述的定理等价于关于 $E^{(n)}$ 的 2- 部分 Birch-Swinnerton-Dyer 猜想. 此定理前半部分的证明完全与文献 [15,16] 相同. 再注意到等式 (1.1), 可知

$$Ш(E^{(n)}/\mathbb{Q})[2^\infty]=0,$$

从而下述定理中最后的等式成立.

定理 1.3 令 $n\equiv 5\ (\mathrm{mod}\ 8)$ 是按照定理 1.2 给出的正整数. 通过复参数化映射, 点

$$(4-4\sqrt{-n})^{-1}\in\mathcal{H}$$

的像 $P_0\in E^{(n)}(\mathbb{C})$ 定义在 $\mathbb{Q}(\sqrt{-n})$ 的 Hilbert 类域 H 上. 进一步地, Heegner 点

$$P:=\sum_{\sigma\in\mathrm{Gal}(H/\mathbb{Q}(\sqrt{-n}))}P_0^\sigma$$

属于 $E^{(n)}(\mathbb{Q})$. 令 $\mu(n)$ 表示 n 的素因子个数, 则

$$P\in 2^{\mu(n)-1}E^{(n)}(\mathbb{Q})+E^{(n)}(\mathbb{Q})_{\mathrm{tor}},$$

但是

$$P\notin 2^{\mu(n)}E^{(n)}(\mathbb{Q})+E^{(n)}(\mathbb{Q})_{\mathrm{tor}}.$$

特别地, P 是无穷阶元素. 进一步地, Mordell-Weil 群 $E^{(n)}(\mathbb{Q})$ 的秩为 1, 并且存在 $u\in\mathbb{Z}_2^\times$ 使得

$$[E^{(n)}(\mathbb{Q}):\mathbb{Z}P+E^{(n)}(\mathbb{Q})_{\mathrm{tor}}]=u\cdot 2^{\mu(n)-1}\cdot\sqrt{|Ш(E^{(n)}/\mathbb{Q})|}.$$

例 1.1 考虑素数 $p=1493\equiv 5\ (\mathrm{mod}\ 8)$, Mordell-Weil 群 $E^{(p)}(\mathbb{Q})$ 模去其挠子群的商群有一个生成元

$$\left[\frac{1674371133}{744769},\ -\frac{51224214734700}{642735647}\right],$$

Heegner 点 $P=(x,y)$ 的横、纵坐标分别为

$$x=\frac{24561535499147214939689754594226969327289514983716301314 53}{29585011828542075719444686875619200646812053585105 29},$$

$$y=\frac{12172578066826359687361812381055798397237566018418043946536533570990618109872158526010 0}{16091910960547986287175324647321077268221974568783910945697471178779686889283 3}.$$

因此

$$Ш(E^{(p)}/\mathbb{Q})\cong(\mathbb{Z}/3\mathbb{Z})^2.$$

设 E 是定义在 $\mathbb{Q}$ 上带复乘的椭圆曲线, 其复乘域为虚二次域 K. 取定奇素数 p 使得 E 在 p 处有潜在好通常约化. 我们知 p 在 K 中是分裂的, 并且不整除 K 中单位根的个数 w_K.

假设 $L(s,E)$ 在 $s=1$ 处有单零点. 由文献 [3] (或者文献 [9]) 中的主定理的结论, 可以选取另一个虚二次域 $\mathcal{K}$ 满足:

(i) p 在 $\mathcal{K}$ 分裂;

(ii) $L(s,E/\mathcal{K})$ 在 $s=1$ 处仍然有单零点.

令 η 是对应于二次扩张 $\mathcal{K}/\mathbb{Q}$ 的二次特征, η_K 是其在 K 上的限制. 令 $E^{(\mathcal{K})}$ 是 E 由二次扩张 $\mathcal{K}/\mathbb{Q}$ 给出的扭变, 则

$$L(1, E^{(\mathcal{K})}) \neq 0.$$

设 $\mathbb{Q}_\infty$ 是 $\mathbb{Q}$ 的分圆 $\mathbb{Z}_p$- 扩张, 并且记 $\Gamma = \mathrm{Gal}(\mathbb{Q}_\infty/\mathbb{Q})$. 对 Γ 的任意一个有限阶特征 ν, 用 $\nu_{\mathcal{K}}$ 表示其在 $\mathrm{Gal}(\mathcal{K}\mathbb{Q}_\infty/\mathcal{K})$ 上的限制. 考虑等式

$$L(s, E \otimes \nu)L(s, E^{(\mathcal{K})} \otimes \nu) = L(s, E_{\mathcal{K}} \otimes \nu_{\mathcal{K}})$$

以及其在 $s = 1$ 处取值, 令 $\mathscr{L}_\varphi$ 和 $\mathscr{L}_{\varphi\eta_K}$ 分别为对应于 E 和 $E^{(\mathcal{K})}$ 的由 Katz 定义的双变元的 p- 进 L- 函数在分圆方向的限制. 记 $\mathscr{L}_{E/\mathcal{K}}$ 是 E 在 $\mathcal{K}$ 上的 p- 进 Rankin-Selberg L- 函数在分圆方向的限制. 为了得到关于 E 的 Birch-Swinnerton-Dyer 猜想, 需要下列证明要点:

(1) 由 Rubin 的关于 K 的双变元的 Iwasawa 主猜想 [13], 可将 $Ш(E/K)[p^\infty]$ 的阶转化成 $\mathscr{L}'_\varphi(1)$. 这里用到了下述事实: 对奇素数 p, 有

$$\mathrm{ord}_p(|Ш(E/K)|) = 2\mathrm{ord}_p(|Ш(E/\mathbb{Q})|).$$

(2) 应用复的 Gross-Zagier 公式 [19] 和 p- 进的 Gross-Zagier 公式 [7], 可得 $\mathscr{L}'_{E/\mathcal{K}}(1)$ 和 $L'(1, E/\mathcal{K})$ $= L'(1, E/\mathbb{Q})L(1, E^{(\mathcal{K})}/\mathbb{Q})$ 之间的精确等式.

(3) 由复的 L- 函数之间的等式以及各 p- 进 L- 函数的插值性质, 我们证明了 $\mathscr{L}'_\varphi(1)\mathscr{L}_{\varphi\eta_K}(1)$ 和 $\mathscr{L}'_{E/\mathcal{K}}(1)$ 之间的精确等式以及 $\mathscr{L}_{\varphi\eta_K}(1)$ 和 $L(1, E^{(\mathcal{K})}/\mathbb{Q})$ 之间的精确等式.

假设 E 在 p 处有坏约化, 但是有潜在好约化; 令 $\mathfrak{p}$ 是 K 中在 p 之上的一个素理想. 那么存在 K 上的椭圆曲线 E' 在 $\overline{K}$ 上同构于 E, 其在 $\mathfrak{p}$ 处有好约化. 除了上述 3 个证明要点外, 在主定理的证明过程中, 还需要比较 E 和 E' 的周期及递降等.

本文余下内容的结构如下. 第 2 节证明 E 在 K 上的 p- 进 Birch-Swinnerton-Dyer 猜想, 并完成上述要点中第一步的具体证明细节. 第 3 节研究复的和 p- 进的 Gross-Zagier 公式, 除了得到两类求导值之间的精确等式外, 还得到一个精确版本的 p- 进 Gross-Zagier 公式. 第 4 节给出前两节中导数值间的精确联系, 并给出主定理 1.1 的证明.

下面给出本文用到的记号:

• 固定一个导子为 $\mathbb{Z}_p$ 的非平凡加性特征 $\psi : \mathbb{Q}_p \to \mathbb{C}_p^\times$. 对于任意特征 $\chi : \mathbb{Q}_p^\times \to \mathbb{C}_p^\times$, 若其导子为 p^n $(n \geqslant 0)$, 则按如下定义根数:

$$\tau(\chi, \psi) = p^{-n} \int_{v_p(t)=-n} \chi^{-1}(t)\psi(t)dt,$$

其中 dt 是 $\mathbb{Q}_p$ 上满足 $\mathrm{Vol}(\mathbb{Z}_p, dt) = 1$ 的 Haar 测度.

• 固定嵌入: $\iota_\infty : \overline{\mathbb{Q}} \hookrightarrow \mathbb{C}$ 和 $\iota_p : \overline{\mathbb{Q}} \hookrightarrow \mathbb{C}_p$ 使得 $\iota_p = \iota \circ \iota_\infty$, 其中 $\iota : \mathbb{C} \xrightarrow{\sim} \mathbb{C}_p$ 是域的同构.

• 设 E 是数域 F 上的椭圆曲线. 假设 E 在 p 之上的所有素理想处有潜在好通常约化, 用 $(\cdot,\cdot)_\infty$ (相应地, $(\cdot,\cdot)_p$) 来记正规化后的 Néron-Tate 高度配对 (相应地, 关于分圆特征的 p- 进高度配对). 若 $P_1, \ldots, P_r \in E(F)$ 构成了 $E(F) \otimes_{\mathbb{Z}} \mathbb{Q}$ 的一组基, 则相应的正则化子定义为

$$R_\infty\left(\frac{E}{F}\right) = \frac{\det((P_i, P_j)_\infty)_{r\times r}}{[E(K) : \sum_i \mathbb{Z}P_i]^2}, \quad R_p\left(\frac{E}{F}\right) = \frac{\det((P_i, P_j)_p)_{r\times r}}{[E(K) : \sum_i \mathbb{Z}P_i]^2}.$$

• 记 $\widehat{\mathbb{Z}} = \prod_p \mathbb{Z}_p$. 对于任意 $\mathbb{Z}$- 代数 R, 记 $R^\times$ 是 R 中可逆元组成的群, $\widehat{R} = R \otimes \widehat{\mathbb{Z}}$.

• 对 $\widehat{K}^\times$ 的特征 χ, 记其导子为 $\mathfrak{f}_\chi \subset \mathcal{O}_K$. 对虚二次域 K, E 是 K 上的带复乘 K 的椭圆曲线, 记 $\mathfrak{f}_E \subset \mathcal{O}_K$ 为其导子.

• 对 K 的非零整理想 $\mathfrak{g}$ 和 $\mathfrak{a}$, 记 $\mathfrak{g}^{(\mathfrak{a})}$ 为 $\mathfrak{g}$ 的与 $\mathfrak{a}$ 互素的部分.

• $\mathbb{D}$ 是 $\mathbb{Z}_p$ 的极大非分歧扩张的完备化, 对于任意有限阶特征 χ, 记 $\mathbb{D}_\chi$ 是 $\mathbb{D}$ 的由 χ 的取值生成的有限扩张.

• L_∞/K 是一个 Abel 扩张, 其 Galois 群 $\mathcal{G} = \mathrm{Gal}(L_\infty/K)$ 同构于 $\Delta \times \Gamma$, 其中 Δ 是有限群, 且 $\Gamma \cong \mathbb{Z}_p^d$. 对于任意 $\mathbb{D}[[\mathcal{G}]]$- 模 M 和 Δ 的特征 χ, 记 $M_\chi = M \otimes_{\mathbb{D}[[\mathcal{G}]],\chi} \mathbb{D}_\chi[[\Gamma]]$. 如果 $p \nmid |\Delta|$, 用 M^χ 表示它的 χ- 分支, 这是 M 的一个直和因子.

• 记 ord_p 是 $\mathbb{C}_p$ 上的满足 $\mathrm{ord}_p(p) = 1$ 的正规加法赋值. 对于任意 $a, b \in \mathbb{C}_p^\times$, 用 $a \sim b$ 表示 $\mathrm{ord}_p(a/b) = 0$.

• 对于有限集合 W, 记 $|W|$ 为其元素个数; 对于任意交换群 G 和任意正整数 m, 记 G_m 是其阶整除 m 的所有元素组成的子群, $G_{\mathrm{tor}} = \bigcup_m G_m$ 为其挠子群.

2 Katz 的 p- 进 L- 函数和分圆 p- 进公式

令 K 是一个虚二次域, E 是定义在 K 上并且带复乘 K 的椭圆曲线. 记 φ 是 E 对应的 Hecke 特征, 则 $\mathfrak{f}_E$ 也是 φ 的导子. 令 p 是一个与 w_K 互素的素数. 假设 p 在 K 中分裂, 即 $p\mathcal{O}_K = \mathfrak{p}\mathfrak{p}^*$, 其中 $\mathfrak{p}$ 为由 ι_p 诱导的素理想. 特别地, 在 $\mathbb{C}_p$ 中, 有 $K_\mathfrak{p} = \mathbb{Q}_p$; 在这个等同下, 记 $K_\mathfrak{p}$ 的加性特征为 $\psi_\mathfrak{p} = \psi_p$. 设 $\Omega_{E/K}$ 是 E 在 K 上的一个 $\mathfrak{p}$- 极小周期, $\varphi_\mathfrak{p}$ 是 φ 的 $\mathfrak{p}$ 分支.

对于 K 中整理想 $\mathfrak{a}$ 和 $\mathfrak{b}$, 令 $K(\mathfrak{a})$ 是 K 的模 $\mathfrak{a}$ 的射线类域, 并记

$$K(\mathfrak{a}\mathfrak{b}^\infty) = \bigcup_{n \geqslant 1} K(\mathfrak{a}\mathfrak{b}^n).$$

定理 2.1 (双变元 p- 进 L- 函数) 令 $\mathfrak{g}$ 是 K 中任意与 p 互素的非零整理想, 假设 $\mathfrak{f}_E^{(p)} \mid \mathfrak{g}$. 那么 $\mathscr{G} = \mathrm{Gal}(K(\mathfrak{g}p^\infty)/K)$ 上存在唯一的测度 $\mu_\mathfrak{g} = \mu_{\mathfrak{g},\mathfrak{p}}$, 使得对于 $\mathscr{G}$ 的任意 $(1,0)$ 型特征 ρ, 有

$$\rho(\mu_\mathfrak{g}) = \frac{\tau(\rho_\mathfrak{p}, \psi_\mathfrak{p})}{\tau(\varphi_\mathfrak{p}, \psi_\mathfrak{p})} \cdot \frac{1 - \rho(\mathfrak{p})p^{-1}}{1 - \overline{\rho(\mathfrak{p})}p^{-1}} \cdot \frac{L^{(\mathfrak{g}p)}(\overline{\rho}, 1)}{\Omega_{E/K}}.$$

这里 $L^{(\mathfrak{g}p)}(\overline{\rho}, s)$ 是 $\overline{\rho}$ 的不包含整除 $\mathfrak{g}p$- 处 Euler 因子的 L- 级数.

注意到, 对于任何 $\mathscr{G}$ 上的特征 $\rho : \mathscr{G} \to \mathbb{C}_p^\times$, 由连续性和线性扩张, 得到一个代数同态

$$\rho : \mathbb{D}[[\mathscr{G}]] \to \mathbb{C}_p,$$

注意到 $\mu_\mathfrak{g} \in \mathbb{D}[[\mathscr{G}]]$, 定理中的 $\rho(\mu_\mathfrak{g})$ 便是 $\mu_\mathfrak{g}$ 在该同态的像. 另外, 上述定理中特征 ρ 型的约定同文献 [6].

证明 这可以由引理 2.1 以及 Yager [18] 和 de Shalit [6] 关于 Katz 的双变元 p- 进测度的构造得到. 此处的测度就是文献 [6, 定理 II.4.14] 中的测度, 其构造方法是 Coates 和 Wiles [5] 利用椭圆单位构造 p- 进 L- 函数的双变元推广. 注意 E 有潜在通常好约化, 利用引理 2.1 将文献 [6, 定理 II.4.14] 的插值公式中的周期代换成了 E 的周期 $\Omega_{E/K}$. □

令 F 是 K 的一个有限 Abel 扩张, 并令 $\Delta=\mathrm{Gal}(F/K)$. 假设 $p\nmid|\Delta|$, 并记 $\mathfrak{f}_{F/K}$ 为 F 的导子 (也是 F/K 的相对判别式). 令 $\mathcal{G}=\mathrm{Gal}(F(E[p^\infty])/K)$, 则 $\mathcal{G}\cong\mathcal{G}_{\mathrm{tor}}\times\Gamma_K$, 其中

$$\Gamma_K=\mathrm{Gal}(F(E[p^\infty])/F(E[p])).$$

令 $\Lambda=\mathbb{Z}_p[[\mathcal{G}]]$ 为 $\mathcal{G}$ 的 Iwasawa- 代数. 记 U_∞ 和 C_∞ 分别是由 $F(E[p^\infty])$ 的在 $\mathfrak{p}$ 上局部主单位和椭圆单位的闭包构成的 Λ- 模 (详细定义参见文献 [13, 第 4 节]). Yager [18] (也可参见文献 [13]) 证明了商模 U_∞/C_∞ 是有限生成的挠 Λ- 模, 记 $\mathrm{Char}_\Lambda(U_\infty/C_\infty)$ 为其特征理想. 因为 $p\nmid|\mathcal{G}_{\mathrm{tor}}|$, 所以任意特征 $\chi:\mathcal{G}_{\mathrm{tor}}\to\mathbb{C}_p^\times$ 的取值都在 $\mathbb{D}^\times$ 中.

定理 2.2 [18] 对于 $\mathcal{G}_{\mathrm{tor}}$ 的任意特征 χ, 令 $\mathfrak{f}=\mathfrak{f}_\chi^{(p)}$. 假设 $\mathfrak{f}_E^{(p)}\mid\mathfrak{f}$. 定义

$$\mu_{\mathfrak{f}}^\chi:=\chi(\mu_{\mathfrak{f}})\in\mathbb{D}[[\Gamma_K]],$$

则有

$$\mathrm{Char}_\Lambda(U_\infty/C_\infty)_\chi\cdot\mathbb{D}[[\Gamma_K]]=(\mu_{\mathfrak{f}}^\chi),$$

其中测度 $\mu_{\mathfrak{f}}$ 由定理 2.1 确定.

引理 2.1 设 E/K 是对应于 Hecke 特征 φ 的椭圆曲线, p 在 K 中分裂, $p\mathcal{O}_K=\mathfrak{p}\mathfrak{p}^*$. 令 φ_0 是 K 的一个 $(1,0)$ 型并在 $\mathfrak{p}$ 处非分歧的 Hecke 特征, 令 $\Omega_{E/K}$ 和 Ω_0 分别为 E 和 φ_0 的 $\mathfrak{p}$- 极小周期. 那么

$$\mathrm{ord}_p\left(\frac{\Omega_{E/K}\cdot\tau(\varphi_{\mathfrak{p}},\psi_{\mathfrak{p}})}{\Omega_0}\right)=0.$$

证明 这由关于 Gauss 和的素理想分解的 Stickelberger 定理可得. 事实上, 对于 $\mathfrak{p}\nmid w=w_K$, E 的 $\mathfrak{p}$- 极小 Weierstrass 方程有如下形式:

$$E:y^2=x^3+a_2x^2+a_4x+a_6,\quad a_2,a_4,a_6\in K^\times\cap\mathcal{O}_{\mathfrak{p}}.$$

若 $w=4,6$, 则可以进一步假设方程形式分别为 $y^2=x^3+a_4x$ 和 $y^2=x^3+a_6$. 那么存在 K 上的椭圆曲线 E' 在 $\overline{K}$ 上同构于 E, 并且 E' 在 $\mathfrak{p}$ 处有好约化. 令 φ' 是其对应的 Hecke 特征, 则存在 $d\in K^\times/K^{\times w}$, 使得 $\epsilon=\varphi\varphi'^{-1}:\mathbb{A}_K^\times/K^\times\to\mathcal{O}_K^\times$ (通过类域论, 也可以视作 Galois 特征) 满足 $\epsilon(\sigma)=\sigma(d^{1/w})/d^{1/w}$. 进而 E' 有在 $\mathfrak{p}$- 处好约化的模型

$$E':\begin{cases}y^2=x^3+da_2x^2+d^2a_4x+d^3a_6, & \text{若 } w=2,\\ y^2=x^3+da_4x, & \text{若 } w=4,\\ y^2=x^3+da_6, & \text{若 } w=6.\end{cases}$$

容易验证 $\Omega_{E'/K}=d^{1/w}\cdot\Omega_{E/K}$.

接下来考虑 Gauss 和的 p- 进赋值. 令 $\omega:\mathcal{O}_{\mathfrak{p}}^\times\to\mu_w\subset K^\times$ 为由 $\omega(a)\equiv a\pmod{\mathfrak{p}}$ 所确定的特征, $\chi=\omega^{-(p-1)/w}$, 则存在 $k\in\mathbb{Z}/w\mathbb{Z}$ 使得 $\epsilon_{\mathfrak{p}}|_{\mathcal{O}_{\mathfrak{p}}^\times}=\chi^k$. 令 $\kappa_{\mathfrak{p}}\cong\mathbb{F}_p$ 为 $K_{\mathfrak{p}}$ 的剩余类域, 则由 Stickelberger 定理知, Gauss 和 $g(\epsilon_{\mathfrak{p}},\psi):=-\sum_{a\in\kappa_{\mathfrak{p}}^\times}\epsilon_{\mathfrak{p}}(a)\psi(a)$ 的 $\mathfrak{p}$- 进赋值为 $\{k/w\}$, 其中 $\{k/w\}$ 是 k 在 $\mathbb{Z}$ 中代表元除以 w 后的非负小数部分. 现在约化到证明 $k=\mathrm{ord}_{\mathfrak{p}}(d)$. 注意到, 对于任意 $u\in\mathcal{O}_{\mathfrak{p}}^\times$, $K_{\mathfrak{p}}(u^{1/w})$ 在 $K_{\mathfrak{p}}$ 上都是非分歧的, 即对 $K_{\mathfrak{p}}$ 的任意素元 π, 都有

$$\sigma_u(\pi^{1/w})/\pi^{1/w}\equiv u^{-(p-1)/w}\pmod{\mathfrak{p}},\quad\forall\,u\in\mathcal{O}_{\mathfrak{p}}^\times.$$

利用局部类域论, 上述断言可以由对应于 $x^p-\pi x$ 的形式群得到.

对于 K 的在 $\mathfrak{p}$ 处非分歧的 Hecke 特征 φ_0 (不需要取值在 K 中) 和它的 $\mathfrak{p}$- 极小周期 Ω_0, 显然有 $\mathrm{ord}_{\mathfrak{p}}(\Omega_0/\Omega_{E'/K})=0$. □

令 μ_{p^∞} 是由 p 的任意指数次单位根组成的群. 由 Weil 配对知 μ_{p^∞} 包含在 $K(E[p^\infty])$ 中. 通过 $\mathcal{G}$ 在 μ_{p^∞} 上的 Galois 作用, 得到 $\mathcal{G}$ 上的 p- 进分圆特征

$$\chi_{\mathrm{cyc},K}:\mathcal{G}\to\mathbb{Z}_p^\times.$$

定义

$$\mathscr{L}_{\varphi_E}(s):=\varphi_E\chi_{\mathrm{cyc},K}^{1-s}(\mu_{\mathfrak{f}_E^{(\mathfrak{p})}}),\quad \forall\, s\in\mathbb{Z}_p.$$

注意到这里将 φ_E 看作是 $\mathcal{G}$ 上的 Galois 特征.

由 Rubin 的双变元 Iwasawa 主猜想能够证明如下定理.

定理 2.3 设 E 是 K 上带复乘 K 的椭圆曲线, φ 是 E 对应的 Hecke 特征. 假设素数 p 与 w_K 互素, 并且 p 在 K 中分裂, 即 $p\mathcal{O}_K=\mathfrak{p}\mathfrak{p}^*$. 令 $r=\mathrm{rank}_K(E(K)\otimes_{\mathcal{O}_K}K)$. 假设 $Ш(E/K)[p^\infty]$ 有限, 且 E 在 K 上的 p- 进高度配对非退化, 则

(1) $\mathscr{L}_\varphi(s)$ 和 $\mathscr{L}_{\overline{\varphi}}(s)$ 在 $s=1$ 处都恰好有 r 阶零点.

(2) 若进一步假设当 $w_K=4$ 或者 $w_K=6$ 时, E 在 $\mathfrak{p}$ 和 $\mathfrak{p}^*$ 同时有好约化或者同时有坏约化; 则对 E/K, p- 进 Birch-Swinnerton-Dyer 猜想成立, 即

$$\mathrm{ord}_p(|Ш(E/K)|)=\mathrm{ord}_p\bigg(\frac{\mathscr{L}_\varphi^{(r)}(1)\mathscr{L}_{\overline{\varphi}}^{(r)}(1)}{R_p(E/K)}\cdot\prod_{v\,|\,p}((1-\varphi_E(v))(1-\overline{\varphi_E(v)}))^{-2}\bigg).$$

进一步地, 若 E 定义在 $\mathbb{Q}$ 上, 则有

$$\mathrm{ord}_p(|Ш(E/\mathbb{Q})|)=\mathrm{ord}_p\bigg(\frac{\mathscr{L}_\varphi^{(r)}(1)}{R_p(E/\mathbb{Q})}\cdot\prod_{v\,|\,p}((1-\varphi_E(v))(1-\overline{\varphi_E(v)}))^{-1}\bigg).$$

证明 设 ϵ 是 K 上满足 $\varphi'=\varphi\epsilon$ 在 $\mathfrak{p}$ 和 $\mathfrak{p}^*$ 处同时非分歧并且取值在 $\mathcal{O}_K^\times$ 中的 Galois 特征. 设 E' 是 K 上对应于 Hecke 特征 φ' 的椭圆曲线, 则 E' 是 E 的 ϵ- 扭变. 那么 E' 在 p 之上都有好约化. 设 F 是 ϵ 的核的固定域, 则 F 是 K 的 Abel 扩张并且 $[F:K]|w_K$. 进一步地, 因为 E 和 E' 在 F 上是同构的, 并注意到 $p\nmid w_K$, 所以有 $E'(F)^{(\epsilon)}\cong E(K)$ 且 $Ш(E'/F)[p^\infty]^{(\epsilon)}\cong Ш(E/K)[p^\infty]$. 令 $F_0=F(E[p])$, 利用 $\mathrm{Gal}(F_0/K)$ 在 $E[p]$ 上的作用, 得到特征 $\chi:\mathrm{Gal}(F_0/K)\to\mathcal{O}_{\mathfrak{p}}^\times$.

令 $F_\infty=F(E[p^\infty])$, $M_{\infty,\mathfrak{p}}$ 是 F_∞ 的仅在 $\mathfrak{p}$ 之上素理想处分歧的极大 Abel p- 扩张. 记

$$X_{\infty,\mathfrak{p}}=\mathrm{Gal}\bigg(\frac{M_{\infty,\mathfrak{p}}}{F_\infty}\bigg).$$

回忆 U_∞ 和 C_∞ 分别表示由 F_∞ 在 $\mathfrak{p}$ 处的局部主单位和椭圆单位生成的 $\Lambda=\mathbb{Z}_p[[\mathrm{Gal}(F_\infty/K)]]$- 模 (如文献 [13] 的第 4 节中的定义). 按照定理 2.2 之前所述以及文献 [13] 中的标准事实可知 $X_{\infty,\mathfrak{p}}$ 和 U_∞/C_∞ 都是有限生成的挠 Λ- 模. 对于有限生成的挠 Λ- 模 $\mathcal{M}$, 记 $\mathrm{Char}_\Lambda(\mathcal{M})$ 为其特征理想. 由 Rubin 的双变元 Iwasawa 主猜想可知

$$\mathrm{Char}_\Lambda(X_{\infty,\mathfrak{p}}^\chi)=\mathrm{Char}_\Lambda\bigg(\frac{U_\infty}{C_\infty}\bigg).$$

进一步地, 由定理 2.2 可知

$$\mathrm{Char}_\Lambda(X^\chi_{\infty,\mathfrak{p}})\mathbb{D}[[\mathrm{Gal}(F_\infty/F_0)]] = (\mu^\chi_{\mathfrak{f}_E^{(p)},\mathfrak{p}}), \tag{2.1}$$

其中对于 K 中与 p 互素的整理想 $\mathfrak{g}$, 测度 $\mu_\mathfrak{g}$ 由定理 2.1 给出.

令 $\mathrm{Sel}(F_\infty, E[\mathfrak{p}^\infty])$ 是 E 在 F_∞ 上的 $\mathfrak{p}$-Selmer 群, $\mathrm{Sel}(F_\infty, E[\mathfrak{p}^\infty])^\vee$ 是其 Pontryagin 对偶. 那么 $\mathrm{Sel}(F_\infty, E[\mathfrak{p}^\infty])^\vee$ 是有限生成的挠 Λ 模, 且

$$\mathrm{Char}_\Lambda(\mathrm{Sel}(F_\infty, E[\mathfrak{p}^\infty])^\vee) = \iota_\mathfrak{p}\mathrm{Char}_\Lambda(X^\chi_{\infty,\mathfrak{p}}), \tag{2.2}$$

其中,

$$\iota_\mathfrak{p} : \Lambda \to \Lambda, \quad \gamma \to \kappa_\mathfrak{p}(\gamma)\gamma, \quad \forall\, \gamma \in \mathrm{Gal}(F_\infty/K).$$

这里, $\kappa_\mathfrak{p}$ 是 $\mathrm{Gal}(F_\infty/K)$ 的由其在 $E[\mathfrak{p}^\infty]$ 的作用决定的特征. 类似地, 也有

$$\mathrm{Char}_\Lambda(X^\chi_{\infty,\mathfrak{p}^*})\mathbb{D}[[\mathrm{Gal}(F_\infty/F_0)]] = (\mu^\chi_{\mathfrak{f}_E^{(p)}\mathfrak{p}^*}) \tag{2.3}$$

和

$$\mathrm{Char}_\Lambda(\mathrm{Sel}(F_\infty, E[\mathfrak{p}^{*\infty}])^\vee) = \iota_{\mathfrak{p}^*}\mathrm{Char}_\Lambda(X^\chi_{\infty,\mathfrak{p}^*}). \tag{2.4}$$

令 F_{cyc} 是 F 的分圆 $\mathbb{Z}_p$ 扩张. 我们知 $\mathrm{Gal}(F_{\mathrm{cyc}}/K) \cong \Delta \times \Gamma$, 其中 $\Delta = \mathrm{Gal}(F/K)$, $\Gamma = \mathrm{Gal}(F_{\mathrm{cyc}}/F)$. 记 $\Lambda_{\mathrm{cyc}} = \mathbb{Z}_p[[\mathrm{Gal}(F_{\mathrm{cyc}}/K)]]$. 用 $\mathrm{Sel}(F_{\mathrm{cyc}}, E[p^\infty])$ 表示 E 在 F_{cyc} 上的 p-Selmer 群, 其 Pontryagin 对偶 $\mathrm{Sel}(F_{\mathrm{cyc}}, E[p^\infty])^\vee$ 是有限生成的挠 Λ_{cyc}- 模, 则有

$$\begin{aligned}\mathrm{Sel}(F_{\mathrm{cyc}}, E[p^\infty]) &= \mathrm{Sel}(F_{\mathrm{cyc}}, E[\mathfrak{p}^\infty]) \oplus \mathrm{Sel}(F_{\mathrm{cyc}}, E[\mathfrak{p}^{*\infty}]) \\ &= \mathrm{Hom}(X_{\infty,\mathfrak{p}}, E[\mathfrak{p}^\infty])^{\mathrm{Gal}(F_\infty/F_{\mathrm{cyc}})} \oplus \mathrm{Hom}(X_{\infty,\mathfrak{p}^*}, E[\mathfrak{p}^{*\infty}])^{\mathrm{Gal}(F_\infty/F_{\mathrm{cyc}})}.\end{aligned}$$

其中第二个等号成立的理由同文献 [13, 定理 12.2], 可由文献 [11, 命题 1.3、定理 1.6 和引理 1.1] 推导出. 对于有限生成的挠 Λ_{cyc}- 模 $\mathcal{M}$, 记 $\mathrm{Char}_{\Lambda_{\mathrm{cyc}}}(\mathcal{M})$ 为其特征理想. 由等式 (2.1)–(2.4) 可知

$$\mathrm{Char}_{\Lambda_{\mathrm{cyc}}}(\mathrm{Sel}(F_{\mathrm{cyc}}, E[p^\infty])^\vee)\mathbb{D}[[\mathrm{Gal}(F_{\mathrm{cyc}}/F)]] = (\iota_\mathfrak{p}\mu^\chi_{\mathfrak{f}_E^{(p)},\mathfrak{p}} \cdot \iota_{\mathfrak{p}^*}\mu^\chi_{\mathfrak{f}_E^{(p)},\mathfrak{p}^*}).$$

回忆 χ_{cyc} 是分圆特征, f_E 是 $\mathrm{Char}_\Lambda(\mathrm{Sel}(F_{\mathrm{cyc}}, E[p^\infty])^\vee)^\Delta$ 的一个生成元, 定义

$$\mathscr{L}(s) = \chi_{\mathrm{cyc}}^{1-s}(f_E), \quad \forall\, s \in \mathbb{Z}_p.$$

则存在取值于 $\mathbb{D}^\times$ 的函数 $u(s)$, 满足

$$\mathscr{L}(s) = u(s)\mathscr{L}_{\varphi_E}(s)\mathscr{L}_{\overline{\varphi_E}}(s), \quad \forall\, s \in \mathbb{Z}_p. \tag{2.5}$$

注意到 $\mathscr{L}_{\varphi_E}(s)$ 和 $\mathscr{L}_{\overline{\varphi_E}}(s)$ 在 $s=1$ 处具有相同的阶, 且两者在 $s=1$ 处的首项系数的乘积在相差一个 p- 进单位下等于 $\mathscr{L}(s)$ 在 $s=1$ 处的首项系数. 由此, 只需要确定 $\mathscr{L}(s)$ 在 $s=1$ 处的阶以及首项系数即可. 由文献 [14] 可知 $\mathscr{L}(s)$ 在 $s=1$ 处的性质由 $\mathrm{Sel}(F_{\mathrm{cyc}}, E[p^\infty])$ 关于 Γ 的广义 Euler 特征决定. 虽然 Schneider[14] 只对 E 在 p 处有好通常约化的情形, 利用等变上同调进行了计算, 但是其关于递降的讨论, 特别是文献 [14, 第 7 节] 中递降图表是 Galois- 等变的. 再注意到 E 在 F 的 p 之上的素位处都有好通常约化, 利用文献 [14] 中同样的方法, 对 E/F 进行递降并取 Δ- 固定部分, 便得到下面的命题.

命题 2.1 令 $r := \mathrm{rank}_K(E(K)\otimes_{\mathcal{O}_K} K)$. 假设 $Ш(E/K)[p^\infty]$ 有限且 $E(K)$ 上的 p- 进高度配对是非退化的, 则 $\mathscr{L}(s)$ 在 $s=1$ 处恰好有 $2r$ 阶零点. 令 $\mathscr{L}^*(1)$ 是它在 $s=1$ 处的首项系数, 则

$$\frac{\mathscr{L}^*(1)}{R_p(E/K)} \sim |Ш(E/K)|\cdot\left|\prod_{v\,|\,p} H^1(\mathrm{Gal}(F(\mu_{p^\infty})/F), E(F(\mu_{p^\infty})\otimes_K K_v))^\Delta\right|^2.$$

引理 2.2 令 $v_0=\mathfrak{p}$ 或者 $v_0=\mathfrak{p}^*$. 假设当 $w_K=4$ 或者 $w_K=6$ 时, E 在 $\mathfrak{p}$ 和 $\mathfrak{p}^*$ 处同时有好约化或者同时有坏约化, 则

$$|H^1(\mathrm{Gal}(F(\mu_{p^\infty})/F), E(F(\mu_{p^\infty})\otimes_K K_{v_0}))^\Delta| \sim (1-\varphi_E(v_0))(1-\overline{\varphi_E(v_0)}).$$

至此完成了定理 2.3 证明. □

本节剩下的部分都是在证明引理 2.2. 注意到文献 [14] 处理了 E 在 p 之上的素位处有好约化的情形, 现在考察 E 在 $\mathfrak{p}$ 或者 $\mathfrak{p}^*$ 处有坏约化的情形. 椭圆曲线 E 和 E' 在 F 上的同构映射给出了同构

$$H^1(\mathrm{Gal}(F(\mu_{p^\infty})/F), E(F(\mu_{p^\infty})\otimes_K K_{v_0}))^\Delta \xrightarrow{\sim} H^1(\mathrm{Gal}(F(\mu_{p^\infty})/F), E'(F(\mu_{p^\infty})\otimes_K K_{v_0}))^\epsilon.$$

由文献 [14, 命题 2] 知, 若 A 是局部域 k 上好通常约化的椭圆曲线, $\widetilde{A}$ 是 A 在 k 的剩余类域 κ 上的约化, 则

$$H^1(\mathrm{Gal}(k(\mu_{p^\infty})/k), A(k(\mu_{p^\infty}))) = |\widetilde{A}(\kappa)[p^\infty]|.$$

令 $w\,|\,v_0$ 是 F 的素位, κ_w 和 κ_{v_0} 分别是 F_w 和 K_{v_0} 的剩余类域, 则有

$$|E'(\kappa_w)| \sim (1-\varphi_{E'}(v_0)^{[\kappa_w:\kappa_{v_0}]})(1-\overline{\varphi_{E'}(v_0)}^{[\kappa_w:\kappa_{v_0}]}).$$

如果 $w_K=2$, 则 F/K 是二次扩张; 如果 E 在 v_0 处有坏约化, 则 F/K 在 v_0 处分歧, 且 w 是 F 在 v_0 之上唯一的素位, 因此有 $\kappa_w=\kappa_{v_0}$, 从而

$$\begin{aligned}|H^1(\mathrm{Gal}(F(\mu_{p^\infty})/F), E'(F(\mu_{p^\infty})\otimes_K K_{v_0}))^\epsilon| &= \frac{|H^1(\mathrm{Gal}(F_w(\mu_{p^\infty})/F_w), E'(F_w(\mu_{p^\infty})))|}{|H^1(\mathrm{Gal}(K_{v_0}(\mu_{p^\infty})/K_{v_0}), E'(K_{v_0}(\mu_{p^\infty})))|}\\ &= \frac{|\widetilde{E'}(\kappa_w)|}{|\widetilde{E'}(\kappa_{v_0})|}\\ &= 1.\end{aligned}$$

若 E 在 v_0 处有好约化, 则 F/K 在 v_0 处是非分歧的. 若 v_0 在 F 中分裂, 则 $F\otimes_K K_{v_0}\simeq K_{v_0}^2$, 且 $\epsilon_{v_0}=1$. 此时显然

$$|H^1(\mathrm{Gal}(F(\mu_{p^\infty})/F), E'(F(\mu_{p^\infty})\otimes_K K_{v_0}))^\epsilon| \sim (1-\varphi_E(v_0))(1-\overline{\varphi_E(v_0)}).$$

若 v_0 在 F 上惯性, 令 w 是 F 在 v_0 之上唯一的素位, 此时由 $\varphi'_{v_0}=\varphi_{v_0}\epsilon_{v_0}$ 和 $\epsilon(v_0)=-1$, 得到

$$\begin{aligned}&|H^1(\mathrm{Gal}(F(\mu_{p^\infty})/F), E'(F(\mu_{p^\infty})\otimes_K K_{v_0}))^\epsilon|\\ &= \frac{|H^1(\mathrm{Gal}(F_w(\mu_{p^\infty})/F_w), E'(F_w(\mu_{p^\infty})))|}{|H^1(\mathrm{Gal}(K_{v_0}(\mu_{p^\infty})/K_{v_0}), E'(K_{v_0}(\mu_{p^\infty})))|}\\ &= \frac{|\widetilde{E'}(\kappa_w)|}{|\widetilde{E'}(\kappa_{v_0})|}\end{aligned}$$

$$\sim \frac{(1-(\varphi\epsilon)(v_0)^2)(1-\overline{\varphi\epsilon(v_0)}^2)}{(1-(\varphi\epsilon)(v_0))(1-\overline{\varphi\epsilon(v_0)})}$$
$$= (1-\varphi(v_0))(1-\overline{\varphi(v_0)})$$

当 $w_K=4$ 或者 $w_K=6$ 时, 由我们的假设可知, v_0 在上 F 分歧, 且 ϵ 在惯性群上非平凡. 证明与之前分歧的情形类似, 这里不再赘述.

3 复的和 p- 进的 Gross-Zagier 公式

假设 E 是 $\mathbb{Q}$ 上导子为 N 的椭圆曲线, ϕ 是 E 对应的新形式. 假设 p 是素数, 且 E 在 p 处有潜在好通常约化或者潜在半稳定约化. 令 $\alpha:\mathbb{Q}_p^\times\to\mathbb{Z}_p^\times$ 是包含于 $(V_pE)^{ss}$ 在 p 处局部表示的特征, 且 $\alpha|_{\mathbb{Z}_p^\times}$ 是有限阶的.

设 $\mathcal{K}$ 是一个满足 $\epsilon(E/\mathcal{K})=-1$ 且 p 在 $\mathcal{K}$ 中分裂的虚二次域. 令 $\Gamma_{\mathcal{K}}$ 是 $\mathcal{K}$ 的 $\mathbb{Z}_p^2$- 扩张的 Galois 群. 由文献 [7] 可知, $\Gamma_{\mathcal{K}}$ 上存在 p- 进测度 $\mu_{E/\mathcal{K}}$ 使得对 $\Gamma_{\mathcal{K}}$ 的任意有限阶特征 χ, 有

$$\chi(\mu_{E/\mathcal{K}})=\frac{L^{(p)}(1,\phi,\chi)}{8\pi^2(\phi,\phi)}\cdot\prod_{w\mid p}Z_w(\chi_w,\psi_w),$$

其中 (ϕ,ϕ) 是 ϕ 的 Petersson 范数

$$(\phi,\phi)=\iint_{\Gamma_0(N)\backslash\mathcal{H}}|\phi(z)|^2dxdy,\quad z=x+\mathrm{i}y;$$

对 $\mathcal{K}$ 的任意素位 $w\mid p$, 令 $\alpha_w=\alpha\circ\mathrm{N}_{\mathcal{K}_w/\mathbb{Q}_p}$, $\psi_w=\psi_p\circ\mathrm{Tr}_{\mathcal{K}_w/\mathbb{Q}_p}$, ϖ_w 是 $\mathcal{K}_w$ 的素元, 则

$$Z_w(\chi_w,\psi_w)=\begin{cases}(1-\alpha_w\chi_w(\varpi_w)^{-1})(1-\alpha_w\chi_w(\varpi_w)p^{-1})^{-1}, & \text{若 } \alpha_w\chi_w \text{ 非分歧},\\ p^n\tau((\alpha_w\chi_w)^{-1},\psi_w), & \text{若 } \alpha_w\chi_w \text{ 导子为 } \varpi_w^n\ (n\geqslant 1).\end{cases}$$

我们需要下面的引理来证明主定理.

引理 3.1 设 E 是定义在 $\mathbb{Q}$ 上带复乘 K 的椭圆曲线. 假设 p 在 K 中分裂, 即 $p\mathcal{O}_K=\mathfrak{p}\mathfrak{p}^*$, 其中 $\mathfrak{p}$ 由 ι_p 诱导, 此时将 $K_{\mathfrak{p}}$ 和 $\mathbb{Q}_p$ 等同; 非平凡元 $\tau\in\mathrm{Gal}(K/\mathbb{Q})$ 诱导了 $\mathbb{A}_K$ 的自同构以及

$$\tau:K_{\mathfrak{p}^*}\xrightarrow{\sim}K_{\mathfrak{p}}=\mathbb{Q}_p.$$

令 φ 是 E 对应的 Hecke 特征, 则有 $\alpha=\varphi_{\mathfrak{p}^*}\circ\tau^{-1}$, 以及对于任意 $x\in\mathbb{Q}_p^\times$, $(\alpha^{-1}\chi_{\mathrm{cyc}})(x)=\varphi_{\mathfrak{p}}(x)x^{-1}$ 都成立. 进一步地, 对于 $\mathcal{K}$ 的任意素位 $w\mid p$ 和任意有限阶特征 $\nu:\widehat{\mathbb{Q}}^\times/\mathbb{Q}^\times\widehat{\mathbb{Z}}^{\times(p)}\mathbb{Z}_{p,\mathrm{tor}}^\times\to\mu_{p^\infty}$, 通过与范数映射的复合将其视作 $\Gamma_{\mathcal{K}}$ 上的特征, 有

$$Z_w(\alpha_w\nu_w,\psi)=\tau(\varphi_{\mathfrak{p}}\nu_p^{-1},\psi)\cdot\frac{1-(\varphi_{\mathfrak{p}}\nu^{-1})(p)p^{-1}}{1-\overline{(\varphi_{\mathfrak{p}}\nu_p^{-1})}(p)p^{-1}}.$$

证明 这个命题直接由 Hecke 特征 φ 的性质 $\varphi\overline{\varphi}=|\cdot|_{\mathbb{A}_K^{(\infty)}}^{-1}$ 和 $\varphi^\tau=\overline{\varphi}$ 得到. □

记 $\Gamma_{\mathcal{K}}$ 的 p- 进分圆特征为 $\chi_{\mathrm{cyc},\mathcal{K}}:\Gamma_{\mathcal{K}}\to\mathbb{Z}_p^\times$, 令 χ 是一个反分圆特征. 定义 p- 进 L- 函数 $\mathscr{L}_{E/\mathcal{K},\chi}$ 如下:

$$\mathscr{L}_{E/\mathcal{K},\chi}(s)=\chi\chi_{\mathrm{cyc},\mathcal{K}}^{s-1}(\mu_{E/\mathcal{K}}),\quad s\in\mathbb{Z}_p.$$

对平凡特征 χ, 记 $\mathscr{L}_{E/\mathcal{K},\chi}$ 为 $\mathscr{L}_{E/\mathcal{K}}$.

定理 3.1 [7, 19] 设 E 是定义在 $\mathbb{Q}$ 上带复乘的椭圆曲线, $\mathcal{K}$ 是虚二次域. 假设 E 在素数 p 处有潜在好通常约化, 且 p 在 $\mathcal{K}$ 上分裂. 假设 $\epsilon(E/\mathcal{K})=-1$, 则

$$\frac{\mathscr{L}'_{E/\mathcal{K},\chi}(1)}{R_p(E/\mathcal{K},\chi)}\cdot\frac{L_p(E/\mathcal{K},\chi,1)}{\prod_{w\,|\,p}Z_w(\chi_w,\psi_w)}=\frac{L'(E/\mathcal{K},\chi,1)}{R_\infty(E/\mathcal{K},\chi)\cdot 8\pi^2(\phi,\phi)},$$

其中 $L_p(E/\mathcal{K},\chi,1)$ 是 p 处的 Euler 因子. 特别地, $\mathscr{L}'_{E/\mathcal{K}}(1)=0$ 当且仅当 $L'(E/\mathcal{K},1)=0$.

证明 令 B 是 $\mathbb{Q}$ 上的非正定四元代数, 其恰好在满足 $\epsilon_v(E/\mathcal{K},\chi)\eta_v(-1)=-1$ 的有限素位 v 处分歧. 众所周知, 存在 $\mathbb{Q}$ 上的具有合适水平的 Shimura 曲线 X 和 $\mathbb{Q}$ 上的非常值映射 $f:X\to E$, 使得 f 将 Hodge 类对应的除子映为 E 的单位元, 由文献 [19, 定理 1.2], 此时的 Heegner 闭链 $P_\chi(f)$ 非挠当且仅当 $L'(E/\mathcal{K},\chi,1)\neq 0$; 另外, 由文献 [7, 定理 B] 和分圆高度配对的非退化性 [1] 可知, Heegner 闭链 $P_\chi(f)$ 非挠当且仅当 $\mathscr{L}'_{E/\mathcal{K},\chi}(1)\neq 0$. 因此 $L'(E/\mathcal{K},\chi,1)=0$ 当且仅当 $\mathscr{L}'_{E/\mathcal{K},\chi}(1)=0$.

假设 $L'(E/\mathcal{K},\chi,1)\neq 0$, 则 $P_\chi(f)$ 是非挠点. 由 Kolyvagin 的 Euler 系方法可知 $(E(\mathcal{K}_\chi)\otimes\mathcal{O}_\chi)^\chi$ 作为 $\mathcal{O}_\chi$- 模的秩是 1, 并且

$$\frac{\widehat{h}_\infty(P_\chi(f))}{R_\infty(E/\mathcal{K},\chi)}=\frac{\widehat{h}_p(P_\chi(f))}{R_p(E/\mathcal{K},\chi)}\in\overline{\mathbb{Q}}^\times.$$

由文献 [19, 定理 1.2] 可知

$$\frac{L'(E/\mathcal{K},\chi,1)}{R_\infty(E/\mathcal{K},\chi)\cdot 8\pi^2(\phi,\phi)}=\frac{\widehat{h}_{NT}(P_\chi(f))}{R_\infty(E/\mathcal{K},\chi)}\cdot\frac{4L(1,\eta)}{\pi c_{\mathcal{K}}}\cdot\frac{L(1,\pi,\mathrm{ad})}{8\pi^3(\phi,\phi)}\alpha^{-1}(f,\chi).$$

再由文献 [7, 定理 B] 和 [8, 附录 B] 可知

$$\frac{\mathscr{L}'_{E/\mathcal{K},\chi}(1)}{R_p(E/\mathcal{K},\chi)}=\frac{h_p(P_\chi(f))}{R_p(E/\mathcal{K},\chi)}\cdot\frac{4L(1,\eta)}{\pi c_{\mathcal{K}}}\cdot\frac{\prod_{w\,|\,p}Z_w(\chi_w,\psi_w)}{L_p(E/\mathcal{K},\chi,1)}\cdot\frac{L(1,\pi,\mathrm{ad})}{8\pi^3(\phi,\phi)}\alpha^{-1}(f,\chi),$$

其中 $\alpha(f,\chi)\in\overline{\mathbb{Q}}^\times$. 至此完成了定理的证明. □

作为应用, 本节给出一个精确版本的 p- 进 Gross-Zagier 公式. 令 χ 的导子为 c, $\mathcal{K}$ 的判别式是 D, 作如下的 Heegner 假设:

(1) $(c,N)=1$, N 没有在 $\mathcal{K}$ 中惯性的素因子, 且若 N 的素因子 q 满足 $q^2\mid N$, 则它在 $\mathcal{K}$ 中分裂;

(2) 对于任意素数 $q\mid(N,D)$, 有 $\chi([\mathfrak{q}])\neq a_q$, 其中, $\mathfrak{q}$ 是 $\mathcal{O}_{\mathcal{K}}$ 中唯一的在 q 之上的素理想, $[\mathfrak{q}]$ 是它在 $\mathrm{Pic}(\mathcal{O}_c)$ 中的理想类.

令 $X_0(N)$ 是 $\mathbb{Q}$ 上的模曲线, 其 $\mathbb{C}$ 点参数化了核为 N 阶循环群的椭圆曲线间的同源 $E_1\to E_2$. 由 Heegner 假设可知, 存在 $\mathcal{O}_c$ 的真理想 $\mathcal{N}$ 满足 $\mathcal{O}_c/\mathcal{N}\cong\mathbb{Z}/N\mathbb{Z}$. 对 $\mathcal{O}_c$ 的任意真理想 $\mathfrak{a}$, 令 $P_{\mathfrak{a}}\in X_0(N)$ 对应于同源 $\mathbb{C}/\mathfrak{a}\to\mathbb{C}/\mathfrak{a}\mathcal{N}^{-1}$. 由复乘理论中的互反律可知, 点 $P_{\mathfrak{a}}$ 定义在 $\mathcal{K}$ 的导子为 c 的环类域 H_c 上, 并且 $P_{\mathfrak{a}}$ 完全由 $\mathfrak{a}$ 在 $\mathrm{Pic}(\mathcal{O}_c)$ 中的类确定. 设 $f:X_0(N)\to E$ 是将尖点 $[\infty]$ 映到单位元 $O\in E$ 模的参数化映射. 记映射 f 的映射度数为 $\deg f$. 定义 Heegner 除子如下:

$$P_\chi(f):=\sum_{[\mathfrak{a}]\in\mathrm{Pic}(\mathcal{O}_c)}f(P_{\mathfrak{a}})\otimes\chi([\mathfrak{a}])\in E(H_c)_{\overline{\mathbb{Q}}}.$$

定理 3.2 令 E 和 χ 选取如上, 并且满足 Heegner 条件 (1) 和 (2). 则

$$L'(1,E,\chi)=2^{-\mu(N,D)}\cdot\frac{8\pi^2(\phi,\phi)_{\Gamma_0(N)}}{u^2\sqrt{|Dc^2|}}\cdot\frac{\widehat{h}_\infty(P_\chi(f))}{\deg f},$$

其中, $\mu(N,D)$ 是 N 和 D 的最大公因子的素因子个数, $u=[\mathcal{O}_c^\times:\mathbb{Z}^\times]$ 是 $\mathcal{O}_c$ 中单位根个数的一半, $\widehat{h}_\infty$ 是 E 在 $\mathcal{K}$ 上的 Néron-Tate 高度. 进一步地, 令 p 是素数, 设 p 在 $\mathcal{K}$ 中分裂且 E 在 p 处有潜在通常约化 (即潜在通常好约化或者潜在半稳定约化), 则有

$$\mathscr{L}'_{E/\mathcal{K},\chi}(1)=\frac{\prod_{w\,|\,p}Z_w(\chi_w,\psi_w)}{L_p(E/\mathcal{K},\chi,1)}\cdot\frac{2^{-\mu(N,D)}}{u^2\sqrt{|Dc^2|}}\cdot\frac{\widehat{h}_p(P_\chi(f))}{\deg f},$$

其中 $\widehat{h}_p$ 是 E 在 $\mathcal{K}$ 上的 p- 进高度.

证明 结合文献 [4] 中的精确 Gross-Zagier 公式和定理 3.1, 可以得到精确 p- 进 Gross-Zagier 公式. □

4 主定理 1.1 的证明

本节回到引言的设定. 设 E 是 $\mathbb{Q}$ 上带复乘 K 的椭圆曲线, Ω_E 是 E 在 $\mathbb{Q}$ 上的最小实周期, $p\nmid w_K$ 是在 K 中分裂的素数. $\Omega_{E/K}$ 是第 2 节中定义的 E 在 K 上的 $\mathfrak{p}$- 极小周期.

引理 4.1 令 $\mathcal{K}$ 是虚二次域, p 在 $\mathcal{K}$ 上分裂, η 是 $\mathcal{K}$ 对应的 $G_\mathbb{Q}$ 的二次特征, η_K 是它在 G_K 上的限制. 假设 $\epsilon(E/\mathcal{K})=-1$, 则存在 p- 进单位 u, 使得

$$\mathscr{L}_{E/\mathcal{K}}=\frac{\tau(\varphi_\mathfrak{p},\psi_\mathfrak{p})^2\cdot\Omega_{E/K}^2}{8\pi^2(\phi,\phi)}\cdot\mathscr{L}_\varphi\mathscr{L}_{\varphi\eta_K}\cdot u.$$

证明 只需要证明, 对于任意有限阶特征 $\nu:\widehat{\mathbb{Q}}/\mathbb{Q}^\times\widehat{\mathbb{Z}}^{\times(p)}\mathbb{Z}_{p,\mathrm{tor}}^\times\to\mathbb{C}^\times$, 有

$$\nu_\mathcal{K}(\mu_{E/\mathcal{K}})=\tau(\varphi_\mathfrak{p},\psi_\mathfrak{p})^2\frac{\Omega_{E/K}^2}{8\pi^2(\phi,\phi)}\cdot\varphi\nu_K^{-1}(\mu_{\mathfrak{f}_0})\cdot\varphi\eta_K\nu_K^{-1}(\mu_{\mathfrak{f}_0}),$$

其中, $\nu_\mathcal{K}=\nu\circ\mathrm{N}_{\mathcal{K}/\mathbb{Q}}$, $\nu_K=\nu\circ\mathrm{N}_{K/\mathbb{Q}}$. 由插值性质可知, 上面待证公式的左边等于

$$\frac{L^{(p)}(1,\phi,\nu_\mathcal{K}^{-1})}{8\pi^2(\phi,\phi)}\prod_{w\,|\,p}Z_w(\alpha_w\nu_w,\psi_w),$$

注意到 $\mathcal{K}/\mathbb{Q}$ 在 p 处分裂, 因此 η_p 平凡. 此时, 上面待证公式的右边等于

$$\frac{\tau(\varphi_\mathfrak{p}\nu_\mathfrak{p}^{-1},\psi_\mathfrak{p})^2}{\tau(\varphi_\mathfrak{p},\psi_\mathfrak{p})^2}\cdot\left(\frac{1-\varphi\nu^{-1}(\mathfrak{p})p^{-1}}{1-\overline{\varphi\nu^{-1}(\mathfrak{p})}p^{-1}}\right)^2\cdot\frac{L^{(p\mathfrak{f}_0)}(\overline{\varphi\nu^{-1}},1)}{\Omega_{E/K}}\cdot\frac{L^{(p\mathfrak{f}_0)}(\overline{\varphi\nu^{-1}\eta_K},1)}{\Omega_{E/K}}.$$

于是由复 L- 函数间的恒等式以及引理 3.1, 便得到了此处的公式. □

现在来证明主定理 1.1. 假设 $L(s,E/\mathbb{Q})$ 在 $s=1$ 处有单零点, 且 E 在 p 处有潜在好通常约化. 令 φ 是 E 对应的 Hecke 特征, $\mathfrak{f}_0$ 是 φ 的导子和 p 互素的部分. 可以取到虚二次域 $\mathcal{K}$ 满足:

- $L(s,E/\mathcal{K})$ 在 $s=1$ 有单零点;
- p 在 $\mathcal{K}$ 中分裂;
- $\mathcal{K}$ 的判别式与 $\mathfrak{f}_0$ 互素.

注意到在这些条件之下, 对应于 p- 进 L- 函数插值的复 L- 函数都是本原 L- 函数, 于是有

$$\mathscr{L}_{\varphi\eta_K}(1)=\frac{L(1,E^{(\mathcal{K})})}{\Omega_{E/K}},$$

$$\frac{\mathscr{L}'_{E/\mathcal{K}}(1)}{R_p(E/\mathcal{K})\tau(\varphi_{\mathfrak{p}},\psi_{\mathfrak{p}})^2}=\frac{L'(E/\mathcal{K},1)}{R_\infty(E/\mathcal{K})8\pi^2(\phi,\phi)},$$
$$\mathrm{ord}_p(|Ш(E/\mathbb{Q})|)=\mathrm{ord}_p\bigg(\frac{\mathscr{L}'_{\varphi}(1)}{R_p(E/\mathbb{Q})}\bigg),$$
$$\mathrm{ord}_p\bigg(\frac{\mathscr{L}'_{E/K}(1)}{\mathscr{L}'_{\varphi}(1)\mathscr{L}_{\varphi\eta_K}(1)}\bigg)=\mathrm{ord}_p\bigg(\frac{\tau(\varphi_{\mathfrak{p}},\psi_{\mathfrak{p}})^2\Omega^2_{E/K}}{8\pi^2(\phi,\phi)}\bigg),$$
$$\mathrm{ord}_p\bigg(\frac{\Omega_{E/K}}{\Omega_E}\bigg)=\mathrm{ord}_p\bigg(\frac{R_p(E/\mathcal{K})}{R_p(E/\mathbb{Q})}\bigg)=0.$$

因此,

$$\mathrm{ord}_p(|Ш(E/\mathbb{Q}|))=\mathrm{ord}_p\bigg(\frac{L'(E/\mathbb{Q},1)}{\Omega_E\cdot R_\infty(E/\mathbb{Q})}\bigg).$$

至此证明了定理 1.1(i).

假设 $E(\mathbb{Q})$ 的秩为 1 且 $Ш(E/\mathbb{Q})[p^\infty]$ 有限, 或者等价地, $E(K)$ 的 $\mathcal{O}_K$- 秩为 1 且 $Ш(E/K)$ 有限. 由文献 [1] 可知分圆高度配对非退化, 所以 $\mathscr{L}_{\varphi_E}$ 和 $\mathscr{L}_{\overline{\varphi_E}}$ 在 $s=1$ 处都恰好有单零点, 从而 $\mathscr{L}_{E/\mathcal{K}}$ 在 $s=1$ 处有单零点. 则从 p- 进 Gross-Zagier 公式可得相关的 Heegner 点的非平凡性, 这就推导出了 $L(E,s)$ 在 $s=1$ 处有单零点. 至此完成了主定理 1.1 的证明.

致谢 作者感谢剑桥大学 John Coates、麦吉尔大学 Henri Darmon 和普林斯顿大学张寿武教授的鼓励.

参考文献

1 Bertrand D. Propriétés Arithmétiques de Fonctions Thêta à Plusieurs Variables. In: Lecture Notes in Mathematics, vol. 1068. Berlin-Heidelberg-New York-Tokyo: Springer, 1984, 17–22
2 Breuil C, Conrad B, Diamond F, et al. On the modularity of elliptic curves over $\mathbb{Q}$: Wild 3-adic exercises. J Amer Math Soc, 2001, 14: 843–939
3 Bump D, Friedberg S, Hoffstein J. Nonvanishing theorems for L-functions of modular forms and their derivatives. Invent Math, 1990, 102: 543–618
4 Cai L, Shu J, Tian Y. Explicit Gross-Zagier and Waldspurger formulae. Algebra Number Theory, 2014, 8: 2523–2572
5 Coates J, Wiles A. On p-adic L-functions and elliptic units. J Aust Math Soc, 1978, 26: 1–25
6 de Shalit E. The Iwasawa Theory of Elliptic Curves with Complex Multiplication. Perspectives in Mathematics, vol. 3. New York: Academic Press, 1987
7 Disegni D. The p-adic Gross-Zagier formula on Shimura curves. Compos Math, 2017, 153: 1987–2074
8 Disegni D. The p-adic Gross-Zagier formula on Shimura curves, II: Nonsplit primes. J Inst Math Jussieu, 2023, 22: 2199–2240
9 Friedberg S, Hoffstein J. Nonvanishing theorems for automorphic L-functions on GL(2). Ann of Math (2), 1995, 142: 385–423
10 Kobayashi S. The p-adic Gross-Zagier formula for elliptic curves at supersingular primes. Invent Math, 2013, 191: 527–629
11 Perrin-Riou B. Groupe de Selmer d'une courbe elliptique à multiplication complexe. Compos Math, 1981, 43: 387–417
12 Perrin-Riou B. Points de Heegner et dérivées de fonctions L p-adiques. Invent Math, 1987, 89: 455–510
13 Rubin K. The "main conjectures" of Iwasawa theory for imaginary quadratic fields. Invent Math, 1991, 103: 25–68
14 Schneider P. Iwasawa L-functions of varieties over algebraic number fields. Invent Math, 1983, 71: 251–293
15 Tian Y. Congruent numbers and Heegner points. Cambridge J Math, 2014, 2: 117–161
16 Tian Y, Yuan X Y, Zhang S W. Genus periods, genus points and congruent number problem. Asian J Math, 2017, 21: 721–774
17 Wiles A. Modular elliptic curves and Fermat's last theorem. Ann of Math (2), 1995, 141: 443–551
18 Yager R I. On two variable p-adic L-functions. Ann of Math (2), 1982, 115: 411–449
19 Yuan X Y, Zhang S W, Zhang W. The Gross-Zagier Formula on Shimura Curves. Annals of Mathematics Studies, vol. 184. Princeton: Princeton Univ Press, 2012

The Birch-Swinnerton-Dyer conjecture of elliptic curves over $\mathbb{Q}$ with complex multiplication

Yongxiong Li, Yu Liu & Ye Tian

Abstract Let E be an elliptic curve over $\mathbb{Q}$ with complex multiplication by K and p be an odd prime such that E has potentially good reduction at p. In this paper, we prove that if $L(s, E)$ has a simple zero at $s = 1$, then the p-part of the Birch-Swinnerton-Dyer conjecture of E holds. Moreover, we give a family of elliptic curves with rank one whose conductors can be divided by any number of primes, satisfying the full Birch-Swinnerton-Dyer conjecture.

Keywords **Birch-Swinnerton-Dyer conjecture, complex multiplication, elliptic curve**

MSC(2020) **11G40**

doi: 10.1360/SSM-2023-0342