中国科学: 数学 2019 年 第 49 卷 第 10 期: 1337 ~ 1346
SCIENTIA SINICA Mathematica
综 述

Iwasawa 理论和 BSD 猜想

献给杨乐教授 80 华诞

万昕

中国科学院数学与系统科学研究院, 北京 100190
E-mail: xwan@math.ac.cn

收稿日期: 2019-04-04; 接受日期: 2019-05-31; 网络出版日期: 2019-08-27
中国科学院青年创新促进会项目 (批准号: Y729025EE1)、国家自然科学基金 (批准号: 11688101 和 11621061) 和中组部青年千人计划及其匹配项目 (批准号: Y7116315K1, Y829091CC1 和 Y750021Z61) 资助项目

摘要 本综述介绍七大千禧年问题之一的 BSD (Birch and Swinnerton-Dyer) 猜想, 以及它的重要研究工具之一 Iwasawa 理论的相关背景. 之后分情形讨论人们对这个问题的研究方法和结果, 着重介绍最近取得的进展.

关键词 Iwasawa 理论 BSD 猜想 代数数论

MSC (2010) 主题分类 11R23

1 简介

本综述简要介绍 Iwasawa 理论和 BSD 猜想的背景理论和一部分近期进展, 以及它们的推广. 我们主要介绍结果和大体的研究思路, 而不追求完全的精确, 并提供相应的参考文献给有兴趣的读者.

2 问题描述

数论中一个中心问题是, 研究解析 L- 函数的特殊值与算术对象之间的关系, 其中一个最经典的问题即数域的类数公式.

2.1 类数公式

假设 K 是有理数域的有限扩张, 记 h_K 为它的理想类数. 记 $L(K,s)$ $(s\in\mathbb{C})$ 为 K 的 Dedekind L-函数. 它是 Riemann zeta 函数对数域的推广. K 的类数公式是如下等式:

$$\mathrm{res}_{s=1}L(K,s)=\frac{2^{r_1}\cdot(2\pi)^{r_2}\mathrm{Reg}_K\cdot h_K}{w_K\sqrt{|D_K|}},\tag{2.1}$$

英文引用格式: Wan X. Iwasawa theory and BSD conjecture (in Chinese). Sci Sin Math, 2019, 49: 1337–1346, doi: 10.1360/N012019-00093

其中 res 是留数, r_1 和 r_2 分别为 K 的实赋值和复赋值的个数, Reg_K 为 K 的正则子 (regulator), w_K 是 K 中的单位根的个数, D_K 是该数域的判别式.

2.2 BSD 猜想

BSD 猜想是 Clay 数学研究所在 2000 年设立的悬赏百万美元求解的千禧年七大难题之一. 它预测了椭圆曲线的算术与它的 L- 函数的解析性质之间的关系. 椭圆曲线是三次方程 $y^2 = x^3 + ax^2 + bx + c$ 定义的光滑三次射影曲线 (记为 E), 其中 x 和 y 是变元, a、b 和 c 是系数. 本文假设 E 定义在有理数域上, 也就是说定义方程的系数为有理数.

椭圆曲线蕴含着丰富的算术信息. 它的一个重要性质是, 其上的点构成一个交换群. 这个群结构由坐标上的有理系数方程定义. 这个椭圆曲线上的有理点集 $E(\mathbb{Q})$ 称为它的 Mordell-Weil 群. 根据 Mordell 的一个著名定理, 这是一个有限生成的交换群. 根据有限生成交换群的结构定理, 它的挠子群 $E(\mathbb{Q})_{\mathrm{tor}}$ 的商群为有限秩 (记为 r_{MW}, 称之为 E 的 Mordell-Weil 秩) 的自由群. 因此, 研究椭圆曲线的 Mordell-Weil 群本质上是研究二元三次不定方程的有理解. 这样就与数论中另一个古老的题目—研究不定方程的解有着密切的关系.

另一方面, 从 E 出发, 我们能够定义一个 Dirichlet 级数 (记为 $L(E,s)$). 它由该椭圆曲线的局部性质 (即在各个素数处的约化) 决定. 根据代数曲线的性质, 这个 Dirichlet 级数在 s 的实部充分大时收敛为一个解析函数. 著名的 Taniyama-Shimura-Weil 猜想的一个等价表述是说, 这个解析函数能够解析延拓为整个复平面上的全纯函数. 这一猜想已经被 Wiles [1]、Taylor 和 Wiles [2] 及 Breuil 等 [3] 证明而成为了一个定理, 其中 Wiles 在 1994 年对该猜想在半稳定椭圆曲线情形的证明推出了著名的 Fermat 大定理, 轰动了世界.

现在介绍 BSD 猜想. 它给出了 $L(E,s)$ 在 $s=1$ (该点称为 L- 函数的中心点) 附近的解析性质的算术解释, 具体如下.

猜想 2.1 (BSD 猜想) (1) (猜想的秩部分) $L(E,s)$ 在 $s=1$ 处的阶 (记为 r) 等于 E 的 Mordell-Weil 秩 r_{MW}.

(2) (完整 BSD 猜想) 我们有如下关于 L- 函数的首项 Taylor 系数的公式:

$$\frac{L^{(r)}(E,1)}{r!\Omega_E R_E} = \frac{\sharp Ш_{E,\mathbb{Q}} \prod_\ell c_\ell(E)}{\sharp(E(\mathbb{Q}))^2_{\mathrm{tor}}}, \tag{2.2}$$

其中 R_E 为 E 的正则子, 它由 Mordell-Weil 群的高度配对的判别式给出 (一般是一个超越数); Ω_E 是椭圆曲线的周期 (一般也是一个超越数); 而 $Ш_{E,\mathbb{Q}}$ 是 Shafarevich-Tate 群 (由一阶的 Galois 上同调定义), 这是一个挠群, Shafarevich-Tate 猜想这是一个有限群, 然而, 在一般情形, 这是一个极其困难的猜想; c_ℓ 是椭圆曲线在 ℓ 处的 Tamagawa 数—这是 E 的一个简单局部不变量.

BSD 猜想与数域的类数公式之间有一个很好的类比: Shafarevich-Tate 群对应于数域的理想类群; Mordell-Weil 群对应于数域的整数环的单位乘法群; Mordell-Weil 秩 r_{MW} 对应于上述单位群的秩 $r_1 + r_2 - 1$; 两种情形的正则子互为类比; Mordell-Weil 群的挠部分对应于数域中的单位根群. BSD 猜想与类数公式一样, 都是揭示解析 L- 函数与算术对象之间一类广泛关系的特殊情形. 这是一种极其深刻的关系.

2.3 Selmer 群

为了研究上述问题, 一个初步的观察是, 为了证明两个正有理数相等, 只需要证明对所有的素数 p,

等式两边的 p- 部分相等即可. 因此, 我们可以专注于研究问题的 p- 部分. 在问题的研究中, 有一类密切相关的算术对象, 称为 p- 进 Selmer 群.

首先考虑类数公式的情形. 对于理想类群, 我们可以用 Galois 上同调的语言给出一个新的定义 (即 Selmer 群):

$$\mathrm{Sel}_K(\mathbb{Q}_p/\mathbb{Z}_p) := \mathrm{Ker}\left\{H^1(K,\mathbb{Q}_p/\mathbb{Z}_p) \to \prod_v \frac{H^1(K_v,\mathbb{Q}_p/\mathbb{Z}_p)}{H^1_f(K_v,\mathbb{Q}_p/\mathbb{Z}_p)}\right\},$$

这里 v 跑遍所有 K 的素理想; H^1 是一阶 Galois 上同调; $\mathbb{Q}_p/\mathbb{Z}_p$ 上的 Galois 群作用定义为平凡作用; 定义

$$H^1_f(K,\mathbb{Q}_p/\mathbb{Z}_p) := \mathrm{Ker}\{H^1(K_v,\mathbb{Q}_p/\mathbb{Z}_p) \to H^1(I_v,\mathbb{Q}_p/\mathbb{Z}_p)\},$$

其中 I_v 为 v 的惰性子群. 根据类域论的基本定理, 容易看出上述定义的 Selmer 群典则同构于理想类群的 p- 部分的对偶.

下面考虑 BSD 猜想的情形. 记 $E[p^\infty]$ 为椭圆曲线的 p^∞ 挠点的集合. 它作为交换群同构于两个 $\mathbb{Q}_p/\mathbb{Z}_p$ 的直和, 并自带一个 $\mathbb{Q}$ 的 Galois 群的自然作用, 定义 E 的 p- 进 Selmer 群如下:

$$\mathrm{Sel}_{\mathbb{Q}}(E[p^\infty]) := \mathrm{Ker}\left\{H^1(\mathbb{Q},E[p^\infty]) \to \prod_v \frac{H^1(\mathbb{Q}_v,E[p^\infty])}{H^1_f(\mathbb{Q}_v,E[p^\infty])}\right\},$$

其中 $H^1_f(\mathbb{Q}_v,E[p^\infty])$ 定义为 Kummer 映射下 $\varinjlim_n E/p^nE$ 的像.

Selmer 群和 BSD 猜想的关系可以从正合列 $0 \to E(\mathbb{Q})\otimes\mathbb{Q}_p/\mathbb{Z}_p \to \mathrm{Sel}_{\mathbb{Q}}(E[p^\infty]) \to Ш_{E,\mathbb{Q}}[p^\infty] \to 0$ 看出. 如果 $Ш_{E,\mathbb{Q}}$ 是一个有限群 (即 Shafarevich-Tate 猜想), 那么从这个正合列可以看出 Mordell-Weil 群的秩应该等于 Selmer 群的秩.

注 2.1 事实上, 解析 L- 函数与 p- 进 Selmer 群之间的关系被 Bloch-Kato 推广到了非常一般的情形. 这称为 Bloch-Kato 猜想 [4].

从某种意义上来说, 目前人们对 Selmer 群的研究已经比较系统化 (相对于 Mordell-Weil 群和 Shafarevich-Tate 群而言). 主要原因是, 在 Langlands 纲领的观点下, 与 L- 函数相联系的自守形式一边与和 Selmer 群联系的 Galois 表示一边存在一种广泛的对偶关系. 因而, 人们能通过自守形式这一强有力而具体的工具研究相应的 Bloch-Kato 猜想.

2.4 BSD 猜想的秩部分

由于 Gross-Zagier 公式和 Kolyvagin 的重要工作 [5–7], 在 $r \leqslant 1$ 情形, BSD 猜想的秩部分已经被人们知道了. 此时存在一种系统的构造 Mordell-Weil 群元素的方法, 称为 Heegner 点. 他们的工作还能推出, 此时完整 BSD 公式的左右两边都是正有理数. 然而, 当 r 大于等于 2 时, 人们知道的还非常少. 此时人们甚至不知道 BSD 公式的左边是否是代数数. 本文主要介绍秩为 0 和 1 时的完整 BSD 公式的研究.

3 Iwasawa 理论

Iwasawa 理论是研究 L- 函数与 Selmer 群之间关系在 pro-p 的域扩张塔下, 或者更一般地, 在 p- 进族下的性质.

3.1 理想类群情形

为简单起见, 记 $\mathbb{Q}_\infty/\mathbb{Q}$ 为分圆 $\mathbb{Z}_p$ 域扩张. 这是一个 Galois 扩张, 相应的 Galois 群 $\Gamma := \mathrm{Gal}(\mathbb{Q}_\infty/\mathbb{Q}) \simeq \mathbb{Z}_p$. 定义 Iwasawa 代数 $\Lambda := \mathbb{Z}_p[[\Gamma]]$. 根据定义知, 空间 $\mathrm{Spec}\Lambda$ 参数化了交换群 Γ 的所有特征.

在 20 世纪 50 年代, Iwasawa 研究了理想类群在这个域扩张塔下的性质. 具体而言, 在上述 Selmer 群的语言下, 他考虑了 $\mathrm{Sel}_{\mathbb{Q}_\infty} := \varinjlim_{\mathbb{Q}\subset\mathbb{Q}_n\subset\mathbb{Q}_\infty} \mathrm{Sel}_{\mathbb{Q}_n}(\mathbb{Q}_p/\mathbb{Z}_p)$, 其中过渡 (transfer) 映射由限制映射给出. 再定义它的 Pontryagin 对偶 $X_{\mathbb{Q}_\infty} := \mathrm{Hom}_{\mathbb{Z}_p}(\mathrm{Sel}_{\mathbb{Q}_\infty}, \mathbb{Q}_p/\mathbb{Z}_p)$. 这些群都自带一个 Galois 群 Γ 的自然作用, 从而, $X_{\mathbb{Q}_\infty}$ 是 Iwasawa 代数 Λ 上的一个模. 由理想类群的有限性可以证明, 这个模是有限生成的.

在解析一边, 存在一个元素 $\mathcal{L}_p \in \Lambda$, 称为 Kubota-Leopoldt p- 进 L- 函数. 在 $\phi \in \mathrm{Spec}\Lambda$ 对应 Γ 的有限阶特征 χ_ϕ 时, 它插值了上述的 Hecke 特征 χ_ϕ 的 Dirichlet L- 函数在 $s = 0$ 处特殊值的代数部分. 由数域的类数公式出发, Iwasawa 提出了如下的猜想, 称为 Iwasawa 主猜想.

猜想 3.1 上述模 X 是 Λ 上的挠模, 并且该挠模的特征多项式正好由 p- 进 L- 函数 $\mathcal{L}_p$ 给出.

这里的特征多项式是刻画 Λ- 模的大小的一个量. 这是 Iwasawa 主猜想在最基本的情形的表述. 它比类数公式蕴含着更精细的信息 (即 Λ 模结构).

此后, 这一猜想的叙述还被推广到了一般的全实域上. 相应的 p- 进 L- 函数由 Deligne-Ribet 构造出来 (参见文献 [8, 9]).

3.2 椭圆曲线和模形式情形

在 Iwasawa 之后, Mazur 把 Iwasawa 的思想应用在研究椭圆曲线的算术当中. 与此前一致, 记 $E/\mathbb{Q}$ 为定义在有理数域上的一个椭圆曲线. 对于椭圆曲线, 相应的 Iwasawa 理论更为复杂. 首先假设 E 在素数 p 处的约化是好的, 也就是说该约化依然是一个 (光滑的) 椭圆曲线. 考虑 E 在 p 处的 Hecke 多项式 $X^2 - a_pX + p = 0$, 其中 $a_p = 1 + p - \sharp E(\mathbb{F}_p)$.

定义 3.1 称 E 在 p 处是正规的, 如果上述的 Hecke 多项式的根中有一个与 p 互素, 或者等价地说, 如果 a_p 与 p 互素.

假设 E 在 p 处正规. 类似地, 对前述的 $\mathbb{Q}_n$, 可定义 E 对应该数域的 Selmer 群, 记为 $\mathrm{Sel}_{\mathbb{Q}_n}(E[p^\infty])$. 同样地可以定义 $\mathrm{Sel}_{\mathbb{Q}_\infty}(E[p^\infty]) = \varinjlim_n \mathrm{Sel}_{\mathbb{Q}_n}(E[p^\infty])$. 我们依然定义 $X_{\mathbb{Q}_\infty}$ 为 $\mathrm{Sel}_{\mathbb{Q}_\infty}(E[p^\infty])$ 的 Pontryagin 对偶. 一个简单的事实是, $X_{\mathbb{Q}_\infty}$ 是 Λ 上的有限生成模.

另一方面, 在解析一边, 根据 Taniyama-Shimura-Weil 猜想, E 对应于一个权为 2 的自守尖形式 (a cusp form). 对此, 文献 [10] 构造了相应的 p- 进 L- 函数, 记为 $\mathcal{L}_{E,p}$. 当 χ_ϕ 跑遍 Γ 的有限阶特征时, 它插值了 L- 函数特殊值 $L(E, \chi_\phi, 1)$ 的代数部分.

Mazur 提出了椭圆曲线情形的 Iwasawa 主猜想如下.

猜想 3.2 假设 E 在 p 处的约化是好的并且正规的, 那么 $X_{\mathbb{Q}_\infty}(E[p^\infty])$ 是 Λ 上的一个挠模. 它的特征多项式由 $\mathcal{L}_{E,p}$ 给出.

Mazur 还证明了如下的定理 (称为 Mazur 控制定理).

定理 3.1 保持上述猜想中的假定. 如果 Iwasawa 主猜想成立, 并且 $L(E, 1)$ 不等于 0, 那么完整 BSD 猜想的 p- 部分成立.

事实上, 此后 Iwasawa 理论的陈述由 Greenberg 做了更进一步的推广. 这里简单介绍正规椭圆模形式的情形 (这是椭圆曲线情形的推广). 假设 $f = \sum_{n=1}^\infty a_n q^n$ 是一个权为 k 的尖模形式, 并假设它是 Hecke 代数作用下的特征形式 (eigenform). 设 L 为 $\mathbb{Q}_p$ 上的有限扩张, 包含 f 的所有 Fourier 系数 a_n. 根据 Eichler、Shimura 和 Deligne 的工作, 存在一个对应的 Galois 表示 $\rho_f : G_\mathbb{Q} \to \mathrm{GL}_2(L)$. 记这个两

维的表示空间为 V. 可以证明存在 V 中一个在 $G_{\mathbb{Q}}$ 作用下稳定的格 T (T 是 $\mathcal{O}_L$ 上的一个秩为 2 的自由模). 假设 f 在 p 处是正规的, 也就是说, 假设 a_p 与 p 互素.

与椭圆曲线的情形类似, 我们可以用表示空间 V/T 代替 $E[p^\infty]$, 定义 $\mathbb{Q}$ 上和 $\mathbb{Q}_\infty$ 上的 Selmer 群, 以及它的 Pontryagin 对偶 $X_{\mathbb{Q}_\infty}(V/T)$. 此时, 由于已经没有 Kummer 映射, 我们需要另外给 Selmer 群定义局部条件, 详细的定义参见文献 [11, 第 3.3 小节].

在解析方面, 对于 f, 存在 Manin-Vishik 的 p- 进 L- 函数 $\mathcal{L}_{f,p}$. 从而类似地也可以陈述相应的 Iwasawa 主猜想: $X_{\mathbb{Q}_\infty}(V/T)$ 是 Λ 上的挠模, 并且它的特征多项式由 $\mathcal{L}_{f,p}$ 给出.

注 3.1 在上面的理论中, 对椭圆曲线或者模形式的正规性假设是非常重要的. 没有这个假设, 相应的 p- 进 L- 函数就不在 Iwasawa 代数里面. 另一方面, 如果简单地取对每个 $\mathbb{Q}_n$ 的 Selmer 群的正向极限的 Pontryagin 对偶, 那么得到的 Λ- 模也不一定是挠模. 所以, 在非正规情形下, 必须对这套理论做一些修改.

4 研究方法和结果

对于 Bloch-Kato 猜想和 Iwasawa 理论的研究, 大体上有两种不同的方法: (1) Euler 系的方法, 主要用来证明猜想中 Selmer 群的上界; (2) 自守形式 (所谓 Eisenstein 同余的方法, 即研究 Eisenstein 级数与尖形式之间的同余), 主要用来证明猜想中 Selmer 群的下界.

4.1 正规情形

对于理想类群的情形, 由于我们知道古典的类数公式, 为了证明 Iwasawa 主猜想, 实际上只需要证明 Selmer 群的上界或者下界中的一个即可. 对于有理数域的情形, 相应的主猜想由 Mazur-Wiles 通过研究 Eisenstein 同余的方法得到证明. 后来 Wiles 改进了证明方法, 得到了对于一般的全实数域的情形. 另外, 在有理数域上的情形, Thaine [12] 发现分圆单位能够用来构造 Euler 系, 从而能够给出 $\mathbb{Q}$ 上的 Iwasawa 主猜想的另外一个证明.

另外一种重要的情形是所谓的复乘 (complex multiplication, CM) 的情形. 设 K 为一个虚二次域. 这一情形研究的是 K 上的 Hecke 特征的 Iwasawa 理论. 这一情形也可以用来研究带复乘的椭圆曲线的 BSD 猜想. 由于依然对应一维的 Galois 表示, 此时只需要证明 Selmer 群的某一个界 (上界或者下界) 即可. Rubin [13,14] 研究了另外一类 Euler 系, 称为 "椭圆单位" 的 Euler 系, 并由此证明了虚二次域情形的 Iwasawa 主猜想. Rubin 的工作借鉴了此前 Thaine 和 Kolyvagin 的工作, 以及 Coates-Wiles 对秩为 0 的复乘椭圆曲线的研究, 并把 Euler 系的工具公理化地抽象出来, 写成了一本专著 [15], 将这个工具应用到了不同的框架下. 近几年来, 田野和他的合作者们在复乘椭圆曲线的 Iwasawa 理论和 BSD 猜想的研究中又有了更进一步的发展. 有兴趣的读者可以参看田野本专辑的文章以及相关文献.

本文主要讨论非复乘的情形. 对于模形式对应的 Galois 表示, Kato [16] 利用模曲线上的 K 理论, 从其上具体构造的 Siegel 单位出发, 再利用 p- 进 Hodge 理论构造出一类 Euler 系, 称为 Kato 的 zeta 元素. 这个 Euler 系能够放入 Rubin 的公理化框架中, 并能得出相应模形式对应 Galois 表示的 Selmer 群的上界. 一个值得指出的地方是, Kato 利用它的 zeta 元素给出了一个 Iwasawa 主猜想的表述, 并不需要用到 p- 进 L- 函数, 同时也不需要假设模形式在 p 处正规.

我们着重解释 Selmer 群的下界的证明方法, 即研究 Eisenstein 同余. 它源于 20 世纪 70 年代 Ribet [17] 的一个先驱性的工作 (称为 Ribet 引理). 我们先把主要的论证步骤总结如下. 假设我们需要

研究某个群 G 对应的自守表示 π 的 Iwasawa 理论.

第 1 步 找出一个更大的群, 使得 G 能够实现为这个大群的一个 Levi 子群. 从这个 G 上的自守表示 π 出发, 利用 Langlands 的理论在大群上构造出一族 Eisenstein 级数. 这里指 Hida 族. 通过 Langlands 和 Shahidi 的计算, 得出这族 Eisenstein 级数的常数项由 π 对应的 p- 进 L- 函数给出.

第 2 步 证明构造出来的这族 Eisenstein 级数是 "本原的" (primitive) (具体来说, 就是跟需要研究的 p- 进 L- 函数 "互素"). 这项信息, 结合第 1 步关于常数项的结论, 告诉我们模掉 (modulo) 要研究的这个 p- 进 L- 函数, 这族 Eisenstein 级数同余于某一族大群上的尖形式 (cusp form). 这一步往往是最技术性的一步, 需要很多的技巧和想法.

第 3 步 利用 Langlands 对应中的结论, 把上述同余翻译到 Galois 表示这边: Eisenstein 级数对应于可约的 Galois 表示, 它的其中一个不可约部分刚好是 π 对应的 Galois 表示; 而尖形式对应的 Galois 表示则比 Eisenstein 级数对应的更加不可约. 根据第 2 步中的同余, 我们能够得到对应 Galois 表示的同余. Ribet 的引理能够被推广到一个纯 Galois 表示理论的构造, 称为 "格构造" (lattice construction), 告诉我们, 从可约和不可约 Galois 表示的同余能够构造出足够多 Selmer 群里的元素 (因为它们可以看成 Galois 表示的扩张类), 从而证明出 Iwasawa 主猜想中 Selmer 群的下界.

读者可能已经注意到, 上述的步骤中要用到 p- 进 L- 函数, 从而需要假设自守形式正规. 另一方面, 第 3 步中的 "格构造" 也需要相应的 Galois 表示满足正规情形所具有的类似性质.

这方面的早期工作包含 Mazur-Wiles 和 Wiles 对 $\mathbb{Q}$ 和全实域的主猜想的证明. 这里 G 取成 GL_1, 而更大的群则取成 GL_2. 在这一情形, 上述的第 2 步变得比较简单, 因为 GL_2 的 Eisenstein 级数的 Fourier 系数计算已经理解得非常清楚.

近期的工作中最重要的一个应是 Skinner 和 Urban [11] 对于 p 为奇素数时正规模形式情形对 Iwasawa 主猜想的证明. 上述的 G 取酉群 $\mathrm{U}(1,1)$, 而大群则选择秩为 4 的酉群 $\mathrm{U}(2,2)$. 选取的原因是, $\mathrm{U}(1,1)$ 的自守形式和 GL_2 椭圆模形式大致相同. 而一般的酉群上的 Langlands 对应人们已经了解得很清楚 (由 Michael Harris 的 "书本项目" 以及吴宝珠对基本引理的证明). 这篇长达 277 页的文章非常的技术性, 通过大量的对 $\mathrm{U}(2,2)$ 上 Eisenstein 级数的 Fourier 系数的计算完成上述总结的第 2 步. 这与此前对一维情形的证明大不相同.

除此之外, 还有 Hsieh [18] 对一般的复乘域 (即一般的全实域上的虚二次扩张) 的 Iwasawa 主猜想的证明. 这时, G 取的是一维酉群 $\mathrm{U}(1)$, 而大群则取 $\mathrm{U}(2,1)$. 这个群不是拟分裂的. 因而需要计算 Fourier-Jacobi 系数 (而不仅仅是 Skinner-Urban 情形的 Fourier 系数). Hsieh 的结果推广了 Rubin 的工作.

4.2 非正规情形

我们讨论非正规的模形式的 Iwasawa 理论. 由于技术上的困难, 我们依然假设 p 是一个奇素数. 首先考虑超奇异 (supersingular) 的椭圆曲线 $E/\mathbb{Q}$ 的情形. 根据代数曲线的 Weil 界, 我们得出, 如果 E 在 p 处有超奇异约化, 并且 p 至少是 5, 那么就有 $a_p = 0$. 首先讨论 $a_p = 0$ 的情形. 此时椭圆曲线在 p 处的 Hecke 多项式的两个根分别为 α 和 $\beta = -\alpha$, $\alpha = \sqrt{-p}$. 记 f 为椭圆曲线对应的权为 2 的尖形式. 我们需要考虑 f 的自守表示中在 U_p-Hecke 作用下的特征向量. 记它们为 f_α 和 f_β.

在解析一边, 对于 f_α 或者 f_β, 根据 Amice-Velu 的构造, 依然可以得到 p- 进 L- 函数 $\mathcal{L}_{f_\alpha}$ 和 $\mathcal{L}_{f_\beta}$. 不过它们都不是 Iwasawa 代数中的元素, 而是在更大的一个环中 (即刚性几何中满足单位开圆盘上满足某种增长条件的函数空间). Pollack [19] 对于这一现象的解决方案如下. 他考虑了 $\mathcal{L}_{f_\alpha}$ 和 $\mathcal{L}_{f_\beta}$ 的线

性组合 $\mathcal{L}_{f_\alpha}\pm\mathcal{L}_{f_\beta}$. 此外, Pollack 还考虑了 "半 p- 进的 Log 函数" 如下 (作为在单位开圆盘上收敛的形式幂级数):

$$\log_p^+(1+X)=\frac{1}{p}\prod_{m=1}^{\infty}\frac{\Phi_{2m}(1+X)}{p},\quad \log_p^-(1+X)=\frac{1}{p}\prod_{m=1}^{\infty}\frac{\Phi_{2m-1}(1+X)}{p},$$

其中 Φ_n 指阶数为 p^n 的分圆多项式. 我们有 $p^2\log_p^+(1+X)\log_p^-(1+X)=\log_p(1+X)$, 即是通常定义的 p- 进 Log 函数.

通过比对 Amice-Velu 的 p- 进 L- 函数的插值公式, Pollack 发现 $\mathcal{L}_{f_\alpha}\pm\mathcal{L}_{f_\beta}$ 分别被 $\log_p^{\pm}(1+X)$ 整除. 此外, 将这个因子 (在刚性函数空间内) 除掉以后, 得到的商就落在 Iwasawa 代数里面 (这可以通过研究这些刚性函数的增长性质得出). Pollack 称之为 $\pm$ p- 进 L- 函数 $\mathcal{L}_{E,p}^{\pm}$.

在算术一边, 人们也希望能够得到对应的类似 Pollack 的 $\pm$ 理论. 这由日本数学家 Kobayashi[20] 解决. 他通过研究 Lubin-Tate 群在 p 处的局部理论, 定义了在分圆域扩张塔中椭圆曲线的所谓 $\pm$-Selmer 群, 记为 $X_{E,\pm}$ (这样得到的 Selmer 群比通过 Kummer 映射的像定义的 Selmer 群更小). Kobayashi 提出了一个 $\pm$ 主猜想如下.

猜想 4.1 $X_{E,\pm}$ 是 Λ 上的挠模, 并且它的特征多项式正好由 $\mathcal{L}_{E,p}^{\pm}$ 给出.

Kobayashi 还证明了他的 $+$ 主猜想与 $-$ 主猜想是等价的, 均等价于 Kato 的主猜想 (回顾 Kato 的主猜想并不需要假设正规性).

接下来讨论这一猜想的证明. 我们希望通过研究某种 Eisenstein 同余来证明 Selmer 群的下界. 不过由前所述, 我们并不能简单地沿着 Skinner 和 Urban 的证明思路进行. 为了解释我们的证明思路 (参见文献 [21]), 首先需要一些关于 Greenberg 的工作的背景理论 (参见文献 [22]).

考虑一个 $G_{\mathbb{Q}}$ 的 p- 进 Galois 表示 V, 并记它的秩为 d. 记 $c\in G_{\mathbb{Q}}$ 为复共轭元素. 记 $d^{\pm}$ 为 V 在 c 作用下特征值为 ±1 的子空间维数. 假设 V 作为 $G_{\mathbb{Q}_p}$ 的表示在 p- 进 Hodge 理论意义下是 de Rham 的, 从而也是 Hodge-Tate 的. 因此存在 Hodge-Tate 分解 $V\otimes\mathbb{C}_p\simeq\oplus_i\mathbb{C}_p(i)^{h_i}$, 其中括号中的 i 表示第 i 个 Tate 扭 (twist), 而 h_i 为重数. 我们做如下 p- 进临界性假定 (Deligne 意义下): (1) 假设 d^+ 等于 $\sum_{i>0}h_i$. 此外, Greenberg 还假设了如下的 Panchishkin 条件: (2) 假设存在一个 V 的 d^+ 维子空间 V^+, 使得 $V^+\otimes\mathbb{C}_p=\sum_{i>0}\mathbb{C}_p(i)^{h_i}$. 我们讨论如下的例子, 这对非正规 Iwasawa 理论的研究至关重要.

考虑一个权为 k 的尖形式 f, 以及一个权为 k' 的假设为正规的复乘模形式 g. 考虑 f 和 g 的 Rankin-Selberg 积, 并做适当的 Tate 扭使得相应的 L- 函数特殊值是 Deligne 意义下的临界值 (critical value). 考虑下面两种情形:

情形 1 假设 $k>k'$, 此时可以验证这个 Rankin-Selberg 积满足 Panchishkin 条件当且仅当 f 为正规.

情形 2 假设 $k'>k$, 此时这个 Rankin-Selberg 积总是满足 Panchishkin 条件, 无论 f 正规与否. Greenberg 的重要思想是说, 只要一个 Galois 表示满足 Panchishkin 条件, 那么它的 Iwasawa 理论就与正规情形类似. 具体而言, 相应的 p- 进 L- 函数 (如果存在的话) 就是 Iwasawa 代数里的元素. 另外相应的分圆域扩张塔上的 Selmer 群的正向极限的 Pontryagin 对偶 X 是 Iwasawa 代数上的挠模. 同时, 也可以陈述相应的 Iwasawa 主猜想: X 的特征多项式是由该 Galois 表示的 p- 进 L- 函数给出.

我们证明的主要工具即是上面例子中的情形 2. 我们取一个辅助性的虚二次域 K, 令 f 为 E 对应的权为 2 的尖形式, 而 g 为对应 K 的复乘模形式. 假设 p 在 K 分裂, 从而, g 在 p 处自动为正规. 假设 g 的权大于 2, 从而对于这个 Rankin-Selberg 积, Greenberg 的 Panchishkin 条件总是成立, 并可以陈述 Iwasawa 主猜想.

我们论证的第 1 步是, 证明这个 Rankin-Selberg 积的 Iwasawa 主猜想中 Selmer 群的下界 (参见文献 [23]). 证明方式是通过研究 U(3,1) 的 Eisenstein 同余. 注意, 我们选的秩为 4 的酉群与 Skinner 和 Urban 选择的 U(2,2) 具有不同的指标. 这样做的原因是, U(3,1) 的 Eisenstein 级数的常数项对应的 L- 函数对应上面例子中的情形 2, 而 U(2,2) 则对应例子中的情形 1. 这也说明了为什么在 U(3,1) 的情形中, 我们不需要假设 f 是正规的; 而在 Skinner 和 Urban 的证明里, 正规性的假设是非常重要的.

下面回到 Kobayashi 的 $\pm$ 主猜想. 表面上看来它与 Greenberg 的主猜想在形式上非常不一样. 为了把它与上面的情形 2 的主猜想联系起来, 我们需要一个桥梁. 因此考虑另外一种 Euler 系, 即所谓的 Beilinson-Flach 元素 Euler 系. 它对应两个模形式的 Rankin-Selberg 积. 这个 Euler 系由 Lei 等 [24] 做了系统的研究. 另一方面, Kings 等 [25] 研究了 Beilinson-Flach 元素的精确互反律, 给出了这些元素在复的和 p- 进的正则子映射下的像与 Rankin-Selberg L- 函数之间的关系. 与 Kato 的 zeta 元素不同的是, 如果考虑在分圆域扩张塔下的极限, Kato 的元素在相应 Galois 表示的 Iwasawa 上同调里面, 而 Beilinson-Flach 元素存在的空间则需要在分母上加上一些 p 的次幂, 也就是说, 在域扩张塔下, 它对应的类不是 p- 进有界的. 然而恰恰由于 Beilinson-Flach 元素的这一性质, 才使得 $\pm$ 的主猜想能够等价于上述情形 2 中的 Greenberg 主猜想—我们仿照 Pollack 的 $\pm$ p- 进 L- 函数的构造, 但是对 f_α 和 f_β 对应的 Beilinson-Flach 元素做一个类似的平均, 然后除掉前述的 $\log_p^{\pm}$ 函数. 可以证明我们能得到 p- 进有界的上同调类, 我们称之为 $\pm$ Beilinson-Flach 类. 之后, 我们通过一些局部理论的研究, 可以构造两个 p- 进的正则子映射. 结合此前提到的 Kings-Loeffler-Zerbes 的精确互反律的研究, 我们能够证明 $\pm$ Beilinson-Flach 元素这个整体上同调类在上述两个正则子下, 分别映到 $\pm$ 主猜想和 Greenberg 主猜想对应的 p- 进 L- 函数. 我们应用这一信息以及 Poitou-Tate 整体对偶定理 (参见文献 [15, 第 1.7 小节]), 可以得到 $\pm$ 主猜想和上面情形 2 的 Greenberg 主猜想中的 Selmer 群的下界是基本互相等价的. 这样结合第 1 步就完成了证明.

上面假设了 $a_p = 0$. 然而当 $p < 5$ 时, a_p 可能不等于 0. 这时的局部理论更为复杂. 对此, Sprung 发展了一套 $\flat/\sharp$ 理论, 推广了之前的 $\pm$- 理论, 并证明了此时相应的 $\flat/\sharp$ 主猜想等价于 Kato 的主猜想. 沿着上述的思路, Sprung [26] 证明了这个 $\flat/\sharp$ 主猜想.

这个结果对 BSD 猜想有着重要的推论. 利用 Kim [27] 证明的 Selmer 群控制定理 (Mazur 控制定理的一个变化形式), 以及 Kobayashi [28] 对 p- 进 Gross-Zagier 公式的工作, 它能用来证明在秩为 0 和 1 时超奇异素数处的 BSD 公式 (注意, 当秩为 1 时, 需要用到 Perrin-Riou 的一个早期结果, 即关于超奇异素数时的 p- 进 height 配对是非零. 这一结论在正规素数时还不知正确与否. 因此, 正规情形秩为 1 时, Iwasawa 主猜想不能推出 BSD 公式).

另外一个由此引出的重要结果是关于完整 BSD 猜想, 即我们现在能够证明对很多非复乘椭圆曲线的二次扭无穷族, 完整 BSD 猜想成立 (即对所有 p, 该椭圆曲线 BSD 猜想的 p- 部分成立). 在此之前, 对于非复乘椭圆曲线, 人们只能对有限多个验证完整 BSD 猜想 (办法是用计算机逐个验证). 我们的结果是这方面第一个一般的理论结果. 注意到此时我们必须考虑 $p = 2$ 的情形. 此时, 文献 [29, 30] 证明了某些特殊无穷族中 BSD 公式的 p- 部分.

4.3 秩为 1 的 BSD 公式

本小节介绍关于秩为 1 时的 BSD 公式的近期进展. 我们主要介绍两方面的工作.

第一个是 Zhang [31] 的工作, 他通过证明 Kolyvagin 猜想的一些情形推出了正规情形秩为 1 的

BSD 公式. 与之前类似, 记 K 为一个辅助选取的虚二次域. Kolyvagin 的猜想是说, 由 Heegner 点构造的 Kolyvagin 系 (与 Euler 系密切相关的一个类似概念) 被 p 整除的最大方幂由在 K 中分裂的素数处的局部 Tamagawa 数的乘积给出. Zhang 的证明方法是, 先通过 Bertolini 和 Darmon 发展的一套利用阶群提升 (level raising) 的同余的办法, 一步步地降低 Selmer 群的秩, 然后化归为一个 Selmer 群为平凡的情形. 之后利用秩为 0 情形的 BSD 公式作为一个信息输入, 利用他证明的在阶群提升中 Kolyvagin 系的同余的结果, 倒回去推出初始时的 Kolyvagin 系是 mod p 非零的 (在他的假设下, 这个方幂是 0), 从而推出 Kolyvagin 猜想. 而相应的 BSD 公式是 Kolyvagin 的理论的一个推论.

第二个是 Jetchev 等 [32] 的一项合作工作. 它与 Zhang 的证明走的是完全不同的思路. 在这个证明中, 正规情形和非正规情形能够得到统一证明. 大体步骤如下: 首先利用 Gross-Zagier 公式, 可以把 BSD 公式化归为证明 Heegner 点的指标与 Shafarevich-Tate 群的大小之间的等式; Bertolini 等 [33] (Bertolini-Darmon-Prasanna, 以下简称 BDP) 证明了一个公式, 把 Heegner 点在 p- 进正则子下的像表述为上一节中提到的 p- 进 L- 函数的一个特殊值 (为了方便起见, 我们把这个 p- 进 L- 函数称为 BDP p- 进 L- 函数); 另一方面, 我们之前对 BDP 情形证明了相应的 Iwasawa 主猜想的一个界. 从这可以得出 BDP p- 进 L- 函数的特殊值和相应的 Selmer 群之间的等式. 利用 Bertolini 等 [33] 的公式和 Poitou-Tate 整体对偶 (用以比较 BDP 情形和原始情形的两个不同 Selmer 群), 上述等式可以转化为 Heegner 点的指标与 Shafarevich-Tate 群之间的等式. 而这正是我们所需要的.

最后简要介绍其他已有的和正在进行中的研究:

(1) 对于乘性 (multiplicative) 约化的椭圆曲线, Skinner [34] 证明了相应的 Iwasawa 主猜想. 证明方式是用 Skinner 和 Urban 对正规好约化情形的一个简单修改 (注意到此时椭圆曲线依然是正规的, 因为 $a_p = \pm 1$). 这就推出了在这些素数中秩为 0 时的 BSD 公式.

(2) 同样在乘性约化的情形, Castella [35] 仿照上述我们和 Jetchev、Skinner 的方法, 证明了秩为 1 时候的 BSD 公式.

此外我们还证明了对一般权的模形式的 Iwasawa 主猜想 [36]. 此时我们需要用到另外的局部理论. 在一项正在进行的合作中, 我们和 Jetchev、Skinner 把之前对椭圆曲线秩为 1 时的 BSD 公式也推广到了一般权的模形式上. 我们还有一些项目研究当椭圆曲线或者模形式在 p 处存在坏的分歧 (ramification) 时的 BSD 公式.

总结起来, 对于奇素数 p, 我们已经有了一套系统性的理论证明秩为 0 和 1 情形的模形式的 BSD 公式的 p- 部分. 我们的结果仍然需要做一些假定, 并不能像复乘情形做得那么完备. 对于 $p = 2$ 的情形, 由于 Iwasawa 理论中的技术困难, 我们知道的还比较少. 目前只对某些特殊的族有一些结果.

致谢 本文是献给杨乐先生的 80 岁生日. 我从小喜欢数学, 小时候就在课堂上学习过杨先生和他的同事们的事迹, 深受鼓舞. 之后走上了数学的道路, 对杨先生的学问和学术经历有了进一步的了解, 更是由衷地敬佩. 2016 年, 我在杨先生的推荐引进下回国工作, 得以得到杨先生的当面教诲, 十分幸运. 也感激杨先生对我们青年学者的关怀. 祝杨先生生日快乐, 健康长寿.

参考文献

1 Wiles A. Modular elliptic curves and Fermat's last theorem. Ann of Math (2), 1995, 141: 443–551
2 Taylor R, Wiles A. Ring-theoretic properties of certain Hecke algebras. Ann of Math (2), 1995, 141: 553–572
3 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
4 Bloch S, Kato K. L-functions and Tamagawa numbers of motives. In: The Grothendieck Festschrift Volume I. Boston: Birkhäuser, 1990, 333–400
5 Gross B, Zagier D. Heegner points and derivatives of L-series. Invent Math, 1986, 84: 225–320

6 Kolyvagin V A. On the structure of Shafarevich-Tate groups. In: Algebraic Geometry. Lecture Notes in Mathematics, vol. 1479. Berlin: Springer, 1991, 94–121
7 Kolyvagin V A. On the structure of Selmer groups. Math Ann, 1991, 291: 253–259
8 Mazur B, Wiles A. Class fields of abelian extensions of Q. Invent Math, 1984, 76: 179–330
9 Wiles A. The Iwasawa conjecture for totally real fields. Ann of Math (2), 1990, 131: 493–540
10 Amice Y, Vélu J. Distributions p-adiques associées aux séries de Hecke. Astérisque, 1975, 24–25: 119–131
11 Skinner C, Urban E. The Iwasawa main conjectures for GL_2. Invent Math, 2014, 195: 1–277
12 Thaine F. On the ideal class groups of real abelian number fields. Ann of Math (2), 1988, 128: 1–18
13 Rubin K. More "main conjectures" for imaginary quadratic fields. Centre Recherches Math, 1994, 4: 23–28
14 Rubin K. The "main conjectures" of Iwasawa theory for imaginary quadratic fields. Invent Math, 1991, 103: 25–68
15 Rubin K. Euler Systems. Annals of Mathematics Studies 147. Princeton: Princeton University Press, 2000
16 Kato K. p-adic Hodge theory and values of zeta functions of modular forms. Astérisque, 2004, 295: 117–290
17 Ribet K. A modular construction of unramified p-extension of $\mathbb{Q}(\mu_p)$. Invent Math, 1976, 34: 151–162
18 Hsieh M L. Eisenstein congruence on unitary groups and Iwasawa main conjectures for CM fields. J Amer Math Soc, 2014, 27: 753–862
19 Pollack R. On the p-adic L-function of a modular form at a supersingular prime. Duke Math J, 2003, 118: 523–558
20 Kobayashi S. Iwasawa theory for elliptic curves at supersingular primes. Invent Math, 2003, 152: 1–36
21 Wan X. Iwasawa main conjecture for supersingular elliptic curves and BSD conjecture. ArXiv:1411.6352, 2014
22 Greenberg R. Iwasawa theory and p-adic deformations of motives. In: Motives. Proceedings of Symposia in Pure Mathematics, vol. 55. Providence: Amer Math Soc, 1994, 193–223
23 Wan X. Iwasawa main conjecture for Rankin-Selberg p-adic L-functions. ArXiv:1408.4044, 2014
24 Lei A, Loeffler D, Zerbes S. Euler systems for Rankin-Selberg convolutions of modular forms. Ann of Math (2), 2014, 180: 653–771
25 Kings G, Loeffler D, Zerbes S. Rankin-Eisenstein classes and explicit reciprocity laws. Cambridge J Math, 2017, 5: 1–122
26 Sprung F. The Iwasawa main conjecture for elliptic curves at odd supersingular primes. ArXiv:1610.10017, 2016
27 Kim B D. The plus/minus Selmer groups for supersingular primes. J Aust Math Soc, 2013, 95: 189–200
28 Kobayashi S. The p-adic Gross-Zagier formula for elliptic curves at supersingular primes. Invent Math, 2013, 191: 527–629
29 Zhai S. Non-vanishing theorems for quadratic twists of elliptic curves. Asian J Math, 2016, 20: 475–502
30 Cai L, Li C, Zhai S. On the 2-part of the Birch and Swinnerton-Dyer conjecture for quadatic twists of elliptic curves. ArXiv:1712.01271, 2017
31 Zhang W. Selmer groups and the indivisibility of Heegner points. Cambridge J Math, 2014, 2: 191–253
32 Jetchev D, Skinner C, Wan X. The Birch and Swinnerton-Dyer formula for elliptic curves of analytic rank one. Cambridge J Math, 2017, 5: 369–434
33 Bertolini M, Darmon H, Prasanna K. Generalized Heegner cycles and p-adic Rankin L-series. Duke Math J, 2013, 162: 1033–1148
34 Skinner C. Multiplicative reduction and the cyclotomic main conjecture for GL_2. Pacific J Math, 2016, 283: 171–200
35 Castella F. On the p-part of the Birch-Swinnerton-Dyer formula for multiplicative primes. Cambridge J Math, 2018, 6: 1–23
36 Wan X. Iwasawa main conjecture for non-ordinary modular forms. ArXiv:1607.07729, 2016

Iwasawa theory and BSD conjecture

Xin Wan

Abstract In this survey article, we introduce the backgrounds for BSD (Birch and Swinnerton-Dyer) conjecture—one of the seven millennium problems, and Iwasawa theory, which is a main tool of the study of BSD conjecture. Then we discuss the methods and results to study them, focusing on recent progress.

Keywords **Iwasawa theory, BSD conjecture, algebraic number theory**

MSC(2010) **11R23**

doi: 10.1360/N012019-00093