中国科学: 数学 2019 年 第 49 卷 第 10 期: 1313～1336
SCIENTIA SINICA Mathematica
《中国科学》杂志社
SCIENCE CHINA PRESS
CrossMark
click for updates

综 述

同余数问题与椭圆曲线

献给杨乐教授 80 华诞

田野[1,2,3]

1. 中国科学院大学, 北京 100049;
2. 中国科学院数学与系统科学研究院, 北京 100190;
3. 中国科学院晨兴数学中心, 北京 100190
E-mail: ytian@math.ac.cn

收稿日期: 2019-02-18; 接受日期: 2019-04-18; 网络出版日期: 2019-09-04
国家自然科学基金 (批准号: 11688101 和 11531008) 资助项目

摘要 设 n 为一个模 8 余 5 的正整数, 使得 n 的所有素因子均模 4 余 1 且 $\mathbb{Q}(\sqrt{-n})$ 没有阶为 4 的理想类. 本文引入对 n 的素因子个数的归纳方法, 给出椭圆曲线 $E^{(n)}: ny^2 = x^3 - x$ 上 Heegner 点的非平凡性, 从而给出 n 为同余数的证明 (定理 6.1). 本文还综述对同余椭圆曲线的 Goldfeld 猜想及 BSD 猜想 (Birch 和 Swinnerton-Dyer 猜想) 方面的结果. 一方面, 基于这种归纳方法, Tian 等 (2017) 推广这一结果得到了更多的同余数, 再结合 Smith (2015) 及 Heath-Brown (1994), 本文证明同余数问题的弱 Goldfeld 猜想 (主定理 A). 另一方面, 基于定理 6.1 以及 Li、Liu 和本人 (2019) 的工作, 本文证明完整 BSD 猜想对椭圆曲线 $E^{(n)}$ 成立 (主定理 B). 这样得到了完整 BSD 猜想对无穷多条秩为 1 的椭圆曲线成立.

关键词 同余数 椭圆曲线 BSD 猜想 Goldfeld 猜想 Heegner 点

MSC (2010) 主题分类 11G40, 11G05, 11D25

1 引言

1.1 同余数问题与椭圆曲线

定义 1.1 一个无平方因子的正整数 n 称为同余数, 如果它是一个有理边长直角三角形的面积, 即存在有理数 a、b 和 c 使得

$$a^2 + b^2 = c^2, \quad \frac{1}{2}ab = n.$$

同余数问题 [1] 是指, 给定一个正整数 n, 判断它是否是同余数, 以及对于一个同余数 n, 找出面积为 n 的有理边长直角三角形.

英文引用格式: Tian Y. Congruent number problem and elliptic curves (in Chinese). Sci Sin Math, 2019, 49: 1313–1336, doi: 10.1360/N012019-00054

© 2019《中国科学》杂志社

同余数问题的本质与椭圆曲线的算术紧密相关. 特别地, 其本质是椭圆曲线的 BSD 猜想和 Goldfeld 猜想. 事实上, 如下结论是容易看到的:

命题 1.2 一个正整数 n 是同余数当且仅当同余椭圆曲线 $E^{(n)}: ny^2 = x^3 - x$ 的 Mordell-Weil 秩大于等于 1. 更进一步地, 对一个正整数 n, 下列集合之间存在一个一一对应:

(1) $\{(a,b,c) \in \mathbb{Q}^3 \mid a^2+b^2=c^2, n=ab/2\}$;

(2) $\{(x,y) \in \mathbb{Q}^2 \mid ny^2 = x^3 - x, y \neq 0\}$,

该一一对应通过如下映射给出:

$$(a,b,c) \mapsto \left(\frac{-b}{a+c}, \frac{2}{a+c}\right), \quad (x,y) \mapsto \left(\frac{1-x^2}{y}, \frac{-2x}{y}, \frac{1+x^2}{y}\right).$$

对于一条定义在有理数域 $\mathbb{Q}$ 上的椭圆曲线 E, 有算术方面和解析方面的如下不变量. 在算术方面, 最基本的对象是 E 的 Mordell-Weil 群 $E(\mathbb{Q})$, 它是 E 的有理点在椭圆曲线的加法下构成的 Abel 群. Mordell[2] 在 1922 年证明了 $E(\mathbb{Q})$ 是一个有限生成的 Abel 群, 其秩 $\operatorname{rank}_{\mathbb{Z}} E(\mathbb{Q})$ 称为 E 的 Mordell-Weil 秩, 或者算术秩, 或者直接简称为秩. 而 Mordell-Weil 群的扭部分 $E(\mathbb{Q})_{\mathrm{tor}}$ 是一个有限群, Mazur[3] 在 1977 年给出了它的所有可能结构, 特别地, 它的阶数小于等于 16. 一个更深刻而神秘的算术对象称为 E 的 Shafarevich-Tate 群:

$$Ш(E) := Ш(E/\mathbb{Q}) := \ker\left(H^1(\mathbb{Q}, E(\overline{\mathbb{Q}})) \to \prod_v H^1(\mathbb{Q}_v, E(\overline{\mathbb{Q}}_v))\right),$$

其中 v 跑遍 $\mathbb{Q}$ 的所有素点 (包括无限素点). 人们猜想 E 的 Shafarevich-Tate 群 $Ш(E/\mathbb{Q})$ 是有限群 (参见文献 [4,5]).

在解析方面, 一个基本对象是 E 的 L 函数 $L(E,s)$, 它在 $\mathrm{Re}(s) > 3/2$ 时是通过 Euler 乘积定义的. 由模性定理知, 它在整个复平面上具有解析延拓. 如果记 $\Lambda(E,s) := 2(2\pi)^{-s}\Gamma(s)L(E,s)$ 为 E 的完全 L 函数, 其中 $\Gamma(s)$ 为 Gamma 函数, 则其满足一个中心点为 $s=1$ 的函数方程:

$$\Lambda(E,s) = \epsilon(E) N_E^{1-s} \cdot \Lambda(E, 2-s),$$

其中 N_E 为 E 的导子, 而 $\epsilon(E) = \pm 1$ 称为 E 的根数 (root number), 或者称为 L 函数 $L(E,s)$ 的符号. 我们将 $L(E,s)$ 在 $s=1$ 处的零点阶数称为 E 的解析秩. 显然, 若 $\epsilon(E) = +1$, 则 E 的解析秩为偶数, 否则为奇数 (于是大于等于 1).

椭圆曲线 E 还有其他一些不变量: 周期 $\Omega(E)$、正规子 $R(E)$ 及在素数 ℓ 处的 Tamagawa 数 $c_\ell(E)$ 等. 这些算术量的定义参见文献 [6].

Birch 和 Swinnerton-Dyer 的猜想 (简称 BSD 猜想)[7] 断言椭圆曲线的算术量 (包括 Mordell-Weil 秩在内) 与它的 L 函数之间的深刻联系:

猜想 1.3 (BSD 猜想) 令 E 是一条定义在 $\mathbb{Q}$ 上的椭圆曲线, 则

(i) (BSD 猜想的秩部分) 我们有

$$\operatorname{rank}_{\mathbb{Z}} E(\mathbb{Q}) = \operatorname*{ord}_{s=1} L(E,s).$$

(ii) (精确 BSD 猜想) 记 r 为 $L(E,s)$ 在 $s=1$ 处的零点阶数, 则有

$$\frac{1}{\Omega(E)R(E)} \lim_{s\to 1} \frac{L(E,s)}{(s-1)^r} = \prod_\ell c_\ell(E) \cdot \frac{\# Ш(E)}{(\# E(\mathbb{Q})_{\mathrm{tor}})^2}.$$

特别地, 等式两边都是正有理数. 对于一个素数 p, BSD 公式的 p 部分成立是指上式两边的有理数的 p 进赋值相等.

记 $\#Ш_{\mathrm{an}}(E)$ 为精确 BSD 猜想所预测的 E 的 Shafarevich-Tate 群的大小:

$$\#Ш_{\mathrm{an}}(E) := \frac{(\#E(\mathbb{Q})_{\mathrm{tor}})^2}{\prod_\ell c_\ell(E)} \cdot \frac{1}{\Omega(E)R(E)} \lim_{s\to 1} \frac{L(E,s)}{(s-1)^r}.$$

目前已知的结果是, 如果 $L(E,s)$ 在 $s=1$ 处的零点阶数小于等于 1, 则 BSD 猜想的秩部分成立 (参见文献 [8–10]), 精确 BSD 猜想等式左边是一个正有理数 (即 $\#Ш_{\mathrm{an}}(E)$ 是一个正有理数), 并且对于很多素数 p, BSD 公式的 p 部分成立. 本文将精确构造一族无穷多的椭圆曲线, 其解析秩为 1, 并且精确 BSD 猜想成立 (主定理 B).

对于一条定义在 $\mathbb{Q}$ 上的椭圆曲线 E, 设其由 Weierstrass 方程 $y^2 = x^3 + ax + b$ 所定义, 以及一个非零整数 n, 定义 E 关于 n 的二次扭曲 (也称为 E 关于二次域 $\mathbb{Q}(\sqrt{n})$ 的二次扭曲) 为 $E^{(n)} : ny^2 = x^3 + ax + b$. 记 $\epsilon(n) := \epsilon(E^{(n)})$ 为 $E^{(n)}$ 的根数. 关于 $\mathrm{ord}_{s=1}L(E^{(n)}, s)$ 的变化行为, Goldfeld [11] 提出了如下的猜想 (另外可参见文献 [12]):

猜想 1.4 (Goldfeld 猜想) 在所有使得 $\epsilon(n) = +1$ (分别地, -1) 的无平方因子的正整数 n 中, 存在一个密度为 1 的子集, 使得当 n 在这个子集中时, $\mathrm{ord}_{s=1}L(E^{(n)}, s) = 0$ (分别地, $= 1$).

密度的概念定义如下:

定义 1.5 如果 $\mathcal{D}$ 是一个正整数的子集, $\mathcal{D}'$ 是 $\mathcal{D}$ 的一个子集, 则 $\mathcal{D}'$ 在 $\mathcal{D}$ 中的密度是指下面的极限 (如果存在的话):

$$\lim_{N\to+\infty} \frac{\#\{n \in \mathcal{D}' \mid n < N\}}{\#\{n \in \mathcal{D} \mid n < N\}}.$$

如果不要求子集的密度为 1, 而只是要求正密度, 则有如下所谓的弱 Goldfeld 猜想:

猜想 1.6 (弱 Goldfeld 猜想) 在所有使得 $\epsilon(n)$ 等于 $+1$ (分别地, -1) 的无平方因子的正整数 n 中, 存在一个正密度的子集, 使得当 n 在这个子集中时, $\mathrm{ord}_{s=1}L(E^{(n)}, s) = 0$ (分别地, $= 1$).

本文将证明对于同余椭圆曲线 $y^2 = x^3 - x$, 其弱 Goldfeld 猜想成立 (主定理 A).

注 1.7 回到同余椭圆曲线 $E : y^2 = x^3 - x$ 及其二次扭曲 $E^{(n)} : ny^2 = x^3 - x$. 在 19 世纪中叶, 人们就知道 $E^{(n)}$ 的 L 函数 $L(E^{(n)}, s)$ 与虚二次域 $\mathbb{Q}(\sqrt{-1})$ 上的一个 Hecke 特征的 L 函数相等, 于是, $\epsilon(n)$ 可以容易地计算 (参见文献 [13]). 设 n 为无平方因子的正整数, 则同余椭圆曲线 $E^{(n)}$ 的根数 $\epsilon(n)$ 为

$$\epsilon(n) = \begin{cases} +1, & 若\ n \equiv 1,2,3 \pmod 8, \\ -1, & 若\ n \equiv 5,6,7 \pmod 8. \end{cases}$$

因此, Goldfeld 猜想在同余数问题上的体现如下:

(1) 在所有 $\equiv 5,6,7 \pmod 8$ 的无平方因子的正整数 n 构成的集合中, 存在一个密度为 1 的子集, 使得当 n 在这个子集中时, $L(E^{(n)}, s)$ 在 $s = 1$ 处有一个单零点.

(2) 在所有 $\equiv 1,2,3 \pmod 8$ 的无平方因子的正整数 n 构成的集合中, 存在一个密度为 1 的子集, 使得当 n 在这个子集中时, $L(E^{(n)}, 1) \neq 0$.

与 BSD 猜想结合, 它预测了如下的两个关于同余数的猜想:

(i) 任意模 8 余 5、6 和 7 的正整数都是同余数;

(ii) 同余数在模 8 余 1、2 和 3 的正整数中的密度为 0.

最近, Smith [14] 证明了一个关于 2^∞-Selmer 秩的类似于 Goldfeld 猜想的结果: 对于同余椭圆曲线 $E: y^2 = x^3 - x$, 在所有 $\equiv 5, 6, 7 \pmod 8$ (分别地, $\equiv 1, 2, 3 \pmod 8$) 的无平方因子的正整数 n 构成的集合中, 存在一个密度为 1 的子集, 使得当 n 在这个子集中时, $E^{(n)}$ 的 2^∞-Selmer 秩为 1 (分别地, 为 0). 特别地, 他证明了上面的猜想 (ii) 成立.

1.2 主要结果

我们的一个主要结果 (参见文献 [15,16]) 是如下的关于同余椭圆曲线的弱 Goldfeld 猜想:

主定理 A 设 $E: y^2 = x^3 - x$ 是同余椭圆曲线.

(i) 在所有 $\equiv 5, 6, 7 \pmod 8$ 的无平方因子的正整数 n 构成的集合中, 存在一个密度大于 50% 的精确构造的子集, 使得当 n 在这个子集中时, $L(E^{(n)}, s)$ 在 $s = 1$ 处有一个单零点, 并且 $E^{(n)}$ 的 BSD 公式的 $p = 2$ 部分成立.

(ii) 在所有 $\equiv 1, 2, 3 \pmod 8$ 的无平方因子的正整数 n 构成的集合中, 存在一个密度大于 40% 的精确构造的子集, 使得当 n 在这个子集中时, $L(E^{(n)}, 1) \neq 0$, 并且 $E^{(n)}$ 的 BSD 公式的 $p = 2$ 部分成立.

上面提到的正密度的子集是精确构造的. 我们的另一个主要结果是在上面的 (i) 中, 精确构造其中的一个子集, 使得精确 BSD 猜想成立:

主定理 B 令 $n \equiv 5 \pmod 8$ 为一个无平方因子的正整数, 它的所有素因子都模 4 余 1, 并且使得 $\mathbb{Q}(\sqrt{-n})$ 没有阶为 4 的理想类, 则 n 是一个同余数, 椭圆曲线 $E^{(n)}: ny^2 = x^3 - x$ 的解析秩为 1 并且精确 BSD 猜想成立.

推论 1.8 对任意正整数 k, 都存在无穷多个恰有 k 个素因子的无平方因子的同余数.

证明 令 $k \geqslant 1$ 为正整数, $q, p_1, \ldots, p_{k-1}$ 为两两不同的素数, 满足

(1) $q \equiv 5 \pmod 8$, 以及对任意 i, 有 $p_i \equiv 1 \pmod 8$;

(2) 对任意 i, Legendre 符号 $(\frac{p_i}{q}) = -1$, 以及对任意 $i \neq j$, 有 $(\frac{p_i}{p_j}) = +1$,

则 $n = qp_1 \cdots p_{k-1}$ 满足主定理 B 中的条件. 又由关于算术级数中素数的 Dirichlet 定理可知, 存在无穷多个这样的 n. 因而, 推论成立. □

注 1.9 基于复乘理论, Heegner [17] 引入了一种系统构造椭圆曲线上有理点的方法, 由此证明了任意模 8 余 5 的素数是同余数. 一个自然的问题是, Heegner 的这个结论能否推广到有多个素因子的模 8 余 5 的无平方因子正整数上. 我们的主定理 B 就是这样的一个推广. 其中, BSD 猜想的秩部分以及精确 BSD 猜想的 2 部分是通过归纳方法证明的, 这是作者最早在文献 [15] 中提出来的, 并在文献 [16] 中被推广, 用于证明主定理 A. 第 2 节将简要回顾 Heegner 的证明, 它同时也是我们归纳方法的基础.

注 1.10 主定理 B 证明中的一个重要组成部分是当 p 是潜在好的通常约化 (potentially good ordinary reduction) 素数的情形时的 BSD 公式的 p 部分, 见第 5 节. 与此同时, 我们最近的工作也考虑了当 p 是潜在超奇异约化 (potentially good supersingular reduction) 素数的情形[1)] (参见文献 [18]) 时的 BSD 公式的 p 部分. 由此, 实际上能得到对于主定理 A(i) 中的精确构造的子集, 当 n 在这个子集中时, $E^{(n)}$ 的精确 BSD 猜想成立.

1) Pan J, Tian Y. BSD formula for CM elliptic curves at bad primes. In preparation

1.3 记号

- $\widehat{\mathbb{Z}} = \prod_{p<\infty} \mathbb{Z}_p$, 其中 p 跑遍所有的素数.
- 对任意 $\mathbb{Z}$- 模 M, 记 $\widehat{M} = M \otimes_{\mathbb{Z}} \widehat{\mathbb{Z}}$. 对数域 K, 令 $\mathbb{A}_K$ 是它的 adéle 环, 以及 $\widehat{K} = \mathbb{A}_K^{(\infty)}$ 是 K 的有限 adéle 组成的集合.
- 对数域 K, 记 $\sigma : \widehat{K}^\times \to \mathrm{Gal}(K^{\mathrm{ab}}/K)$ 为 Artin 映射, 并且, 将 K 的理想类群 $\mathcal{A}$ 与 $\widehat{K}^\times/K^\times\widehat{\mathcal{O}}_K^\times$ 等同. 特别地, σ 诱导了同构 $\mathcal{A} \xrightarrow{\sim} \mathrm{Gal}(H/K)$, 其中 H 是 K 的 Hilbert 类域.
- $\mathbb{A} = \mathbb{A}_{\mathbb{Q}}$. 对任意 $\mathbb{Q}$ 上代数群 G, 记 $G_{\mathbb{A}} = G(\mathbb{A})$ 为 G 的 $\mathbb{A}$ 点.
- 对任意 $\mathbb{Z}$- 模 M 和任意正整数 n, 记 $M[n]$ 是 M 被 n 所零化的子群.

2 素数情形: Heegner-Birch 方法

首先看主定理 B 在 n 是一个素数时的情形. 这将是证明主定理 B 归纳方法的起始步骤. 令 E 为 $y^2 = x^3 - x$.

定理 2.1 任意模 8 余 5 的素数 p 都是同余数, 而且 $\#Ш_{\mathrm{an}}(E^{(p)})$ 是一个 2 进单位.

证明 令 $K = \mathbb{Q}(\sqrt{-p})$, H 为 K 的 Hilbert 类域, $H_0 = K(\sqrt{p}) \subset H$. 令 $\mathcal{A} = \widehat{K}^\times/K^\times\widehat{\mathcal{O}}_K^\times$ 为 K 的理想类群, 则在类域论的 Artin 同构 $\sigma : \mathcal{A} \xrightarrow{\sim} \mathrm{Gal}(H/K)$ 下, $2\mathcal{A} \cong \mathrm{Gal}(H/H_0)$ 且由 Gauss 的亏格理论知其为奇数.

我们将定义一个来自 E 的复单值化及复乘理论的点 $z \in E(H)$ (参见定义 6.4 和定理 6.5). 由于复共轭在 $\mathrm{Gal}(H/K)$ 上的作用为取逆, 且在子群 $\mathrm{Gal}(H/H_0)$ 上稳定, 从而, Heegner 点为

$$y_p := \mathrm{Tr}_{H/H_0} z \in E(\mathbb{Q}(\sqrt{p})).$$

对任意 $t \in \widehat{K}^\times$, 记 $\sigma_t z = z_t$. 令 ϖ 为 K_2 (即 K 在 2 处完备化得到的局部域) 的单一化子, 则由复乘理论 (参见定理 6.5), 对任意 $t \in \widehat{K}^\times$, $z_{\varpi t} + z_t = (0,0) \in E[2]$ 为非平凡 2 阶点. 从而,

$$y_p + \sigma_\varpi y_p = \#\mathrm{Gal}(H/H_0) \cdot (0,0) = (0,0).$$

由 $\sigma_\varpi(\sqrt{p}) = -\sqrt{p}$ 可知, $2y_p \in E(\mathbb{Q}(\sqrt{p}))^-$, 但 $y_p \notin E(\mathbb{Q}(\sqrt{p}))^-$, 这里 $E(\mathbb{Q}(\sqrt{p}))^- \subset E(\mathbb{Q}(\sqrt{p}))$ 记在 $\mathrm{Gal}(\mathbb{Q}(\sqrt{p})/\mathbb{Q})$ 中非平凡元素作用下变为负元的元素形成的子群. 注意 $E(\mathbb{Q}(\sqrt{p}))^- \cong E^{(p)}(\mathbb{Q})$. 我们断言 $2y_p \notin 2E(\mathbb{Q}(\sqrt{p}))^- + E[2]$ (从而为无限阶点). 若不然, 则存在点 $y' \in E(\mathbb{Q}(\sqrt{p}))^-$ 和 $Q \in E[2]$ 使得 $2(y_p - y') = Q$. 于是, $y_p - y' \in E[4] \cap E(\mathbb{Q}(\sqrt{p})) = E[2]$.

这样, 我们证明了 p 是一个同余数. 由 Gross-Zagier 公式 (参见定理 6.3) 可知, $E^{(p)}$ 的解析秩为 1 且 $\#Ш_{\mathrm{an}}(E^{(p)})$ 为 2 进单位. □

类似地, 我们也可给出判断一个素数是否是非同余数的方法.

定理 2.2 任意模 8 余 3 的素数 p 都不是同余数, 而且 $\#Ш_{\mathrm{an}}(E^{(p)})$ 是一个 2 进单位.

证明 令 $K = \mathbb{Q}(\sqrt{-p})$, $\mathcal{A}$ 是 K 的理想类群. 由 Gauss 的亏格理论知, $\#\mathcal{A}$ 是奇数.

令 B 是 $\mathbb{Q}$ 上的恰在 2 和 ∞ 处分歧的四元代数. 令 π 为 E 所对应的 $B_{\mathbb{A}}^\times$ 的自守表示 (参见第 6.3 小节对 π 的进一步刻画). 固定一个 K 到 B 的 $\mathbb{Q}$- 嵌入, 以及一个 B 的极大序模 (order) $\mathcal{O}_B$ 使得 $\mathcal{O}_B \cap K = \mathcal{O}_K$. 令 $R = \mathcal{O}_K + 4\mathcal{O}_B$. 令 $U = \widehat{R}^\times$. 嵌入 $K \hookrightarrow B$ 诱导了映射 $\mathcal{A} = K^\times\backslash\widehat{K}^\times/\widehat{\mathcal{O}}_K^\times \to B^\times\backslash\widehat{B}^\times/U$.

考虑 π 中被 U 固定的整数值自守形式全体, 其为一个秩为 1 的自由 $\mathbb{Z}$ 模, 令 $f:\widehat{B}^\times\to\mathbb{Z}$ 为它的一个生成元. 考虑周期

$$y_p=\sum_{t\in\mathcal{A}}f(t).$$

通过精确计算 (如文献 [16, 第 2.2 小节]) 知, f 在 $(\widehat{B}^\times)^2$ 取值都是奇数. 特别地, f 在 $\mathcal{A}=2\mathcal{A}$ 上的取值也是奇数, 从而, y_p 是奇数. 根据 Waldspurger 公式 (参见定理 3.2), $E^{(p)}$ 的解析秩为 0 (由 Coates-Wiles 定理 [8] 知, $E^{(p)}$ 的算术秩也为 0, 从而, p 是一个非同余数) 且

$$y_p^2=[\mathcal{O}_K^\times:\mathbb{Z}^\times]^2\cdot\#Ш_{\mathrm{an}}(E)\cdot\#Ш_{\mathrm{an}}(E^{(p)}).$$

由于 $Ш_{\mathrm{an}}(E)=1$, 因此, $\#Ш_{\mathrm{an}}(E^{(p)})$ 是一个 2 进单位. □

注 2.3 Fermat 在 17 世纪中叶给出了一个 1 不是同余数的初等证明, 这个证明方法被称为无穷递降法. 通过同样的方法, 可以初等地证明任意模 8 余 3 的素数 p 都不是同余数. 事实上, 这同时证明了 $E^{(p)}$ 的 Shafarevich-Tate 群的 2 部分平凡, 因此, 与定理 2.2 结合, 我们知道 $E^{(p)}$ 的 BSD 公式的 2 部分成立. 我们在此简要陈述此初等证明如下.

模 8 余 3 的素数 p 不是同余数的初等证明 假设 $p\equiv 3\pmod 8$ 是同余数, 则存在正整数 r、s 和 t 使得 t 最小, 满足

$$rs(r+s)(r-s)=pt^2. \tag{2.1}$$

由 t 的最小性可知, $2\nmid r+s$, $(r,s)=1$, 于是, r、s、$r+s$ 和 $r-s$ 两两互素, 因此存在正整数 x、y、z 和 w 使得如下四种情形中有一种发生.

(i) $r=px^2$, $s=y^2$, $r+s=z^2$, $r-s=w^2$. 这时有 $y^2+w^2=px^2$. 若 $p\nmid y$, 则 $p\nmid w$, 这与 $(\frac{-1}{p})=-1$ 矛盾. 因此, $p\mid y$, $p\mid w$, 进而, $p\mid x$, $p\mid z$, 与 $(r,s)=1$ 矛盾.

(ii) $r=x^2$, $s=py^2$, $r+s=z^2$, $r-s=w^2$. 考虑 $\frac{z+w}{2}$ 和 $\frac{z-w}{2}$, 它们是两个互素的整数, 因为 z 和 w 都是奇数, 有 $(\frac{z+w}{2})^2+(\frac{z-w}{2})^2=\frac{z^2+w^2}{2}=r=x^2$, 因此在必要时将 w 替换成 $-w$, 可以找到整数 u 和 v 使得 $\frac{z+w}{2}=u^2-v^2$, $\frac{z-w}{2}=2uv$, $x=u^2+v^2$ 成立. 现在有 $uv(u+v)(u-v)=\frac{z-w}{4}\cdot\frac{z+w}{2}=\frac{z^2-w^2}{8}=p(\frac{y}{2})^2$, 因此, $(u,v,\frac{y}{2})$ 也是方程 (2.1) 的正整数解, 这与 t 的最小性矛盾.

(iii) $r=x^2$, $s=y^2$, $r+s=pz^2$, $r-s=w^2$. 这时有 $x^2+y^2=pz^2$, 与 (i) 类似发生矛盾.

(iv) $r=x^2$, $s=y^2$, $r+s=z^2$, $r-s=pw^2$. 这时有 $z^2+pw^2=2x^2$. 若 $p\nmid x$, 则 $p\nmid z$, 这与 $(\frac{2}{p})=-1$ 矛盾. 因此, $p\mid x$, $p\mid z$, 进而, $p\mid y$, $p\mid w$, 与 $(r,s)=1$ 矛盾.

综上所述, (2.1) 没有正整数解, 即 p 不是同余数. □

定理 2.4 令 $p\equiv 3,5\pmod 8$ 是一个素数, 则 BSD 猜想对椭圆曲线 $E^{(p)}:py^2=x^3-x$ 成立.

证明 对 $p\equiv 3\pmod 8$, 由定理 2.2 的证明知, $E^{(p)}$ 的解析秩为 0 且 $\#Ш_{\mathrm{an}}(E^{(p)})$ 是一个 2 进单位. 又由前述 Fermat 的无穷递降法证明了 $E^{(p)}$ 的算术秩为 0 且 $\#Ш(E^{(p)})$ 是一个 2 进单位, 因而, BSD 的秩部分成立且 BSD 公式的 2 部分也成立. 由 Rubin [19] 的结果, $E^{(p)}$ 的 BSD 公式的任意奇素数部分也成立.

对 $p\equiv 5\pmod 8$, 由定理 2.1 的证明知, $E^{(p)}$ 的解析秩为 1 且 $\#Ш_{\mathrm{an}}(E^{(p)})$ 是一个 2 进单位. 再由无穷递降法, 得到 2-Selmer 群模掉 $E^{(p)}[2]$ 得到的 $\mathbb{F}_2$- 线性空间的维数为 1. 又由定理 2.1 的证明得到一个非平凡的 Heegner 点, 因而, $E^{(p)}$ 的算术秩为 1 且 $\#Ш(E^{(p)})$ 是一个 2 进单位. 从而, BSD 的秩部分成立且 BSD 公式的 2 部分也成立. 再由 Perrin-Riou [20] 和 Kobayashi [21] 的工作, 对任意一个奇素数 $q\neq p$, BSD 公式的 q 部分成立. 最后, 由定理 5.1 得到 BSD 公式的 p 部分也成立. □

注 2.5 现在看到, 对同余椭圆曲线 $ny^2 = x^3 - x$, 当 $n \equiv 3, 5 \pmod 8$ 为一个素数时, 其解析秩只能取 0 或 1. 然而, 素数在无平方因子的正整数中的密度为 0. 为了得到 Goldfeld 猜想, 应当进一步考虑有多个素因子的 n. 这时令 $K = \mathbb{Q}(\sqrt{-n})$, 则 K 的理想类数不再是奇数, 上面的 Heegner-Birch 方法不能直接使用. 第 4 节使用所有亏格特征所对应的 Heegner 点, 引入归纳方法来给出一个具有正密度的判别条件. 第 6 节在一个较简单的情形详细展示此归纳方法.

3 精确 Gross-Zagier 公式和 Waldspurger 公式

本文的归纳方法 (参见第 6 节), 在归纳步骤中, 还依赖于精确 Gross-Zagier 公式和精确 Waldspurger 公式. 这是我们在文献 [22] 的工作, 它是原始 Gross-Zagier 公式 [9] 的推广, 是 Yuan 等 [23] 的公式的精确化.

3.1 Gross-Zagier 公式

考虑三元组 (E, K, χ), 其中 E 表示一个定义在 $\mathbb{Q}$ 上的导子为 N 的椭圆曲线; K 表示一个判别式为 D 的虚二次域, 以及 $\eta : \mathbb{A}_{\mathbb{Q}}^{\times}/\mathbb{Q}^{\times} \to \{\pm 1\}$ 是域扩张 $K/\mathbb{Q}$ 所对应的二次特征; $\chi : \mathrm{Gal}(H_c/K) \to \mathbb{C}^{\times}$ 是导子为 c 的环类域 (ring class field) H_c 的一个本原特征, 这里 H_c 是 K 的唯一 Abel 扩展使得 Artin 映射诱导了同构 $\mathrm{Pic}(\mathcal{O}_c) \xrightarrow{\sim} \mathrm{Gal}(H_c/K)$, 其中 $\mathcal{O}_c = \mathbb{Z} + c\mathcal{O}_K$ 是 K 的导子为 c 的序模且 $\mathrm{Pic}(\mathcal{O}_c)$ 是可逆 (分式) $\mathcal{O}_c$- 理想的 Picard 群.

假设 Rankin-Selberg L 函数 $L(s, E, \chi)$ 的符号 $\epsilon(E, \chi)$ 是 -1, 并且假设 $(c, N) = 1$. 令 B 为 $\mathbb{Q}$ 上的不定四元代数, 它在有限素点 v 上分歧当且仅当

$$\epsilon(E_v, \chi_v) = -\chi_v \eta_v(-1),$$

这里 $\epsilon(E_v, \chi_v)$ 是 $L(s, E, \chi)$ 在 v 处的局部根数. 令 R 为 B 的一个判别式为 N 的序模并且在一个固定的嵌入 $K \hookrightarrow B$ 之下满足 $R \cap K = \mathcal{O}_c$. 这样的序模是存在的, 并且在相差一个 $\widehat{K}^{\times}$ 的共轭的意义下唯一. 令 $X_{\widehat{R}^{\times}}$ 为定义在 $\mathbb{Q}$ 上的 B 所对应的 Shimura 曲线, 级为 $\widehat{R}^{\times}$. 它的复点构成一个 Riemann 面, 结构如下:

$$X_{\widehat{R}^{\times}}(\mathbb{C}) \cong B_+^{\times} \backslash \mathcal{H} \times \widehat{B}^{\times}/\widehat{R}^{\times} \cup \{\text{尖点}\},$$

其中 $B_+^{\times}$ 是 $B^{\times}$ 中约化范数为正的元素全体, 它按照一个固定的同构 $B(\mathbb{R}) \cong M_2(\mathbb{R})$ 作用在上半平面 $\mathcal{H}$ 上. 尖点构成的集合非空当且仅当 B 是分裂的. 记 $[z, g]_{\widehat{R}^{\times}}$ 为元素 $(z, g) \in \mathcal{H} \times \widehat{B}^{\times}$ 在 $X_{\widehat{R}^{\times}}(\mathbb{C})$ 中的像.

在曲线 $X_{\widehat{R}^{\times}}$ 上存在一个特别的除子类 $\xi_{\widehat{R}^{\times}} \in \mathrm{Pic}(X_{\widehat{R}^{\times}})_{\mathbb{Q}}$, 它在 $X_{\widehat{R}^{\times}}$ 的每一个连通分支上的次数都是 1. 在模曲线 $X_0(N)$ 的情形, 可以将其取为无穷远处的尖点所对应的除子类. 在一般情形下, 可以将其取为正规化的 Hodge 类, 即一个唯一的线丛, 它在每个几何连通分支上的次数都是 1, 并且与

$$\omega_{X_{\widehat{R}^{\times}}/\mathbb{Q}} + \sum_{x \in X_{\widehat{R}^{\times}}(\overline{\mathbb{Q}})} (1 - e_x^{-1})x$$

平行, 其中 $\omega_{X_{\widehat{R}^{\times}}/\mathbb{Q}}$ 是 $X_{\widehat{R}^{\times}}$ 的典则线丛, e_x 是 x 在 $X_{\widehat{R}^{\times}}$ 的复单值化下的分歧指数, 即如果 x 是尖点, $e_x = \infty$, 则 $1 - e_x^{-1} = 1$; 如果 x 不是尖点, 则 e_x 是 x 在任意一个自然映射 $X_{U'} \to X_{\widehat{R}^{\times}}$ 下的任意一个原像的分歧指数, 这里 U' 是 $\widehat{R}^{\times}$ 的任意一个充分小的紧开子群, 使得任意一个 $X_{U'}$ 的几何连通分支在复单值化下都是上半平面 $\mathcal{H}$ 的一个自由商.

根据模性定理和 Jacquet-Langlands 对应可知, 存在一个 E 被 $X_{\widehat{R}^\times}$ 的模参数化, 这是一个定义在 $\mathbb{Q}$ 上的非常值的态射 $f: X_{\widehat{R}^\times} \to E$, 满足如下的条件:

(1) 它将正规化的 Hodge 类 $\xi_{\widehat{R}^\times}$ 映成 O, 也就是说, 存在一个 $\xi_{\widehat{R}^\times}$ 的非零整数倍, 它被一个整系数的除子 $\sum_i n_i x_i$ 表出, 并且使得在 $E(\mathbb{Q})$ 中 $\sum_i n_i f(x_i) = O$.

(2) 对任意 $p \mid (N, D)$, 有 $T_{\varpi_{K_p}} f = \chi_p^{-1}(\varpi_{K_p}) f$. 对任意素数 $p \mid (N, D)$, $K_p^\times$ 正规化 $R_p^\times$, 一个 K_p 的归一化子 (uniformizer) ϖ_{K_p} 在 Shimura 曲线上的 Hecke 作用诱导了一个定义在 $\mathbb{Q}$ 上的 $X_{\widehat{R}^\times}$ 的自同构 $T_{\varpi_{K_p}}$, 它在 $X_{\widehat{R}^\times}(\mathbb{C})$ 上是由 $[z, g]_{\widehat{R}^\times} \mapsto [z, g \cdot \varpi_{K_p}]_{\widehat{R}^\times}$ 给出的. 注意到对这样的 p 有 $\chi_p(\varpi_{K_p}) = \pm 1$. 更进一步地, 如果 f' 是另一个满足如上条件的模参数化, 则存在非零整数 n 和 n' 使得 $nf = n'f'$. 这称为 "重数一性质".

重数一性质是由下面的局部表示论的结果得到的. 令 $p < \infty$ 是一个有限素点. 令 π_p 为 E 所对应的尖自守表示在 $B_{\mathbb{A}}^\times$ 上的 Jacquet-Langlands 对应的 p 分量, 则

(1) 若 $\mathrm{ord}_p(N_p) \leqslant 1$ 或者 $K_p/\mathbb{Q}_p$ 是非分歧的, 则 π_p 在 $R_p^\times$ 作用下的不变子空间 $\pi_p^{R_p^\times}$ 是一维的.

(2) 若 $\mathrm{ord}_p(N_p) \geqslant 2$ 并且 $K_p/\mathbb{Q}_p$ 是分歧的, 则 $\dim_{\mathbb{C}} \pi_p^{R_p^\times} \leqslant 2$ 而且存在 $\pi_p^{R_p^\times}$ 的一个唯一的一维子空间, 在其之上 $K_p^\times$ 按照 χ_p^{-1} 作用.

令 z_0 为唯一的在上半平面 $\mathcal{H}$ 上被 $K^\times$ 固定的点, 令 P 为 $X_{\widehat{R}^\times}$ 之上在复单值化下被双陪集 $[z_0, 1]_{\widehat{R}^\times}$ 所表示的点, 则 Shimura 互反律告诉我们, $P \in X_{\widehat{R}^\times}(K^{\mathrm{ab}})$, 并且对任意 $t \in \widehat{K}^\times$, 记 $\sigma_t \in \mathrm{Gal}(K^{\mathrm{ab}}/K)$ 为 t 在 Artin 映射 $\sigma: \widehat{K}^\times/K^\times \to \mathrm{Gal}(K^{\mathrm{ab}}/K)$ 之下的像, 则有

$$[z, 1]_{\widehat{R}^\times}^{\sigma_t} = [z, t]_{\widehat{R}^\times}.$$

因此, 根据 $R \cap K = \mathcal{O}_c$, 有 $P \in X_{\widehat{R}^\times}(H_c)$, 其中 H_c 是 K 的导子为 c 的环类域, 即在 Artin 映射下诱导同构 $\mathrm{Gal}(H_c/K) \cong K^\times \backslash \widehat{K}^\times / \widehat{\mathcal{O}}_c^\times$ 的 K 的 Abel 扩张. 定义 Heegner 点

$$P_\chi(f) := \sum_{\sigma \in \mathrm{Gal}(H_c/K)} f(P)^\sigma \chi(\sigma).$$

Gross-Zagier 公式给出了 Heegner 点 $P_\chi(f)$ 的 Néron-Tate 高度与 Rankin-Selberg L 函数 $L(s, E, \chi)$ 在 $s = 1$ 处的一阶导数值 $L'(1, E, \chi)$ 的关系.

定理 3.1 (Gross-Zagier 公式[22]) 假设 (E, χ) 的符号为 -1 并且 $(c, N) = 1$, 则 Heegner 点 $P_\chi(f)$ 满足如下的高度公式:

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

其中 ϕ 是 E 所对应的新形式, 以及它的 Peterson 内积为

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

$u = [\mathcal{O}_c^\times : \mathbb{Z}^\times]$, $\mu(N, D)$ 是 N 和 D 的公共素因子的个数; $\widehat{h}_K$ 是 E 在 K 上的 Néron-Tate 高度; $\deg f$ 是态射 f 的次数.

为了使用本原 Heegner 点, 在第 6 节中, 我们实际上使用了模参数化 $f_0: X_U \to E$, 其中 $U \subset \widehat{R}^\times$ 是一个更小的紧开子群, 使得 f_0 的一个倍数 f 通过 $X_{\widehat{R}^\times}$ 分解, 并且相同的 Gross-Zagier 公式也成立.

3.2 Waldspurger 公式

为了完成我们的归纳方法, 我们还需要 Waldspurger 公式. 我们仍然考虑如前面所述的三元组 (E,K,χ), 但是现在假设 L 函数 $L(s,E,\chi)$ 的符号是 $+1$. 仍然假设 $(c,N)=1$. 与之前类似, 令 B 为 $\mathbb{Q}$ 上的正定四元代数, 它在有限素点 v 上分歧当且仅当 $\varepsilon(E_v,\chi_v)=-\chi_v\eta_v(-1)$. 令 R 为 B 的一个判别式为 N 的序模并且在一个固定的嵌入 $K\hookrightarrow B$ 之下满足 $R\cap K=\mathcal{O}_c$. 现在不再考虑 Shimura 曲线, 转而考虑 Shimura 集 $X_{\widehat{R}^\times}=B^\times\backslash\widehat{B}^\times/\widehat{R}^\times$.

对任意素数 $p\nmid N$, 存在一个作用在自由 Abel 群 $\mathbb{Z}[X_{\widehat{R}^\times}]$ 之上的 Hecke 作用 T_p, 它按如下的方式定义. 对于 $p\nmid N$, 集合 $B_p^\times/R_p^\times\cong\mathrm{GL}_2(\mathbb{Q}_p)/\mathrm{GL}_2(\mathbb{Z}_p)$ 可以视为 $\mathbb{Q}_p$ 上的二维线性空间中的 $\mathbb{Z}_p$- 格的全体, 则对于任意 $g=(g_v)\in\widehat{B}^\times$, 定义

$$T_p([g])=\sum_{h_p}[g^{(p)}h_p], \tag{3.1}$$

其中 $g^{(p)}$ 为 g 去掉 p 的部分, 即 $g^{(p)}=(g_v^{(p)})$, 这里 $g_v^{(p)}=g_v$ 对任意 $v\neq p$ 和 $g_p^{(p)}=1$ 成立; 如果 g_p 对应于一个格 Λ, 则 h_p 跑遍所有 $p+1$ 个子格 $\Lambda'\subset\Lambda$ 使得 $[\Lambda:\Lambda']=p$.

根据 Jacquet-Langlands 对应, 存在一个函数

$$f:X_{\widehat{R}^\times}\to\mathbb{Z}$$

使得对任意 $p\nmid N$, Hecke 算子 T_p 在 f 上按照 a_p 作用, 并且对任意 $p\mid(N,D)$, $\varpi_{K,p}$ 在 f 上的右乘作用 $f(\cdot\varpi_{K,p})=\chi_p(\varpi_{K,p})^{-1}f$. 这样的 f 在相差一个常数倍数的意义下唯一, 该重数一性质由与之前的 Gross-Zagier 公式之中类似的理由给出.

定义环面周期

$$P_\chi(f)=\sum_{\sigma\in\mathrm{Gal}(H_c/K)}f(t)\chi(\sigma),$$

其中 $\mathrm{Gal}(H_c/K)\cong K^\times\backslash\widehat{K}^\times/\widehat{\mathcal{O}}_c^\times\to X_{\widehat{R}^\times}$, $\sigma\mapsto t$ 由固定的嵌入 $K\hookrightarrow B$ 所诱导.

定理 3.2 (Waldspurger 公式[22]) 假设 (E,χ) 的符号为 $+1$ 并且 $(c,N)=1$, 则有

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

在这里, 如果 $f=\sum_i f(g_i)[g_i]$, 其中 $\{[g_i]\}$ 是一个 $X_{\widehat{R}^\times}$ 的代表元集, 则定义

$$\deg f=\sum_i f(g_i)^2w_i^{-1},$$

其中 w_i 是集合 $(B^\times\cap g_i\widehat{B}^\times g_i^{-1})/\{\pm1\}$ 的大小.

4 弱 Goldfeld 猜想

本节将展示如何从我们之前的工作 [15,16] 和 Smith 的工作 [14,24] 导出主定理 A. 为了方便起见, 只证明主定理 A(i), 而主定理 A(ii) 的证明是类似的.

对于一个无平方因子的正整数 n, 若 $E^{(n)}$ 的解析秩小于等于 1, 令 $\mathcal{L}(n)$ 为使 $\mathcal{L}(n)^2=\#Ш_{\mathrm{an}}(E^{(n)})$ 的正实数; 如果 $E^{(n)}$ 的解析秩 $\geqslant 2$, 则定义 $\mathcal{L}(n)=0$.

如果 $E^{(d)}$ 的根数是 -1, 当 $\mathcal{L}(d)\neq 0$ 时, 令 α_d 为 $E(\mathbb{Q}(\sqrt{d}))^-$ 在模掉扭子群的意义下的一个生成元; 当 $\mathcal{L}(d)=0$ 时, 定义 $\alpha_d=0$. 记 $\mathcal{P}(d)=\mathcal{L}(d)\alpha_d$.

对于一个对应于分解 $D=d_0d_1$ 的亏格特征 χ, 即对应于二次扩张 $\mathbb{Q}(\sqrt{d_0},\sqrt{d_1})/K$ 的二次特征, 我们之前提到的 Gross-Zagier 和 Waldspurger 公式在符号 $+1$ 时, 将 $P_\chi(f)$ 和 $\mathcal{L}(d_0)\mathcal{L}(d_1)$ 联系起来, 在符号 -1 时, 将 $P_\chi(f)$ 和 $\mathcal{P}(d_0)\mathcal{L}(d_1)$ 联系起来. 这里选取 d_0 使得 $E^{(d_0)}$ 的根数是 -1.

命题 4.1 令 E 为曲线 $y^2=x^3-x$. 对任意无平方因子的正整数 n, 令 f 为 E 关于平凡特征在 $K_n:=\mathbb{Q}(\sqrt{-n})$ 之上的本原测试向量, 它在相差正负号的意义下唯一 (参见文献 [16]). 令 χ 为 K_n 上的一个非分歧的亏格特征. 令 $h_2(n)$ 为 K_n 的理想类群的 2 秩.

(1) 如果 $n\equiv 1,2,3 \pmod 8$ 并且 $\epsilon(E,\chi)=+1$, 则周期 $P_\chi(f)$ 非零的一个必要条件是, 可以将 n 写为 $n=d_0d_1$, 其中 $0<d_1\equiv 1 \pmod 8$, 使得 χ 是 $K_n(\sqrt{d_1})/K_n$ 所对应的特征. 在这种情形下, 有

$$P_\chi(f)=\pm 2^{h_2(n)-\delta}u_{K_n}\mathcal{L}(d_1)\mathcal{L}(d_2),$$

其中 $\delta=1$, 若 $n\equiv 1 \pmod 8$; $\delta=0$, 若 $n\equiv 2,3 \pmod 8$.

(2) 如果 $n\equiv 5,6,7 \pmod 8$ 并且 $\epsilon(E,\chi)=-1$, 则点 $P_\chi(f)$ 不是扭点的一个必要条件是, 可以将 n 写为 $n=d_0d_1$, 其中 $0<d_0\equiv 5,6,7 \pmod 8$, $0<d_1\equiv 1,2,3 \pmod 8$, 使得当 $n\equiv 5,6 \pmod 8$ 时, $\chi=\chi_{d_0,d_1}$ 是 $K_n(\sqrt{d_1})/K_n$ 所对应的特征; 当 $n\equiv 7 \pmod 8$ 时, $\chi=\chi_{d_0,d_1}$ 是 $K_n(\sqrt{d_1^*})/K_n$ 所对应的特征. 在这种情形下, 有

$$P_\chi(f)=\epsilon(d_0,d_1)2^{h_2(n)}\mathcal{P}(d_0)\mathcal{L}(d_1), \tag{4.1}$$

其中 $\epsilon(d_0,d_1)=\pm\mathrm{i}$, 若 $(d_0,d_1)\equiv(5,3) \pmod 8$; $\epsilon(d_0,d_1)=\pm 1$, 在其他情形下.

此命题的证明要点如下. 设 $d_0\equiv 5,6,7 \pmod 8$ 是一个无平方因子的正整数, 我们想了解 "Heegner 点" $\mathcal{P}(d_0)$ 的信息. 我们想比较它在不同亏格特征 $\chi=\chi_{d_0,d_1}$ 之下的投影 P_χ. 令 $n=d_0d_1$ 和 $n'=d_0d_1'$ 是我们要考虑的两个情形. 选取 e_0 使得 e_0d_1 和 e_0d_1' 在符号为 $+1$ 的情形中. 如果记 $P(d_0,d_1)$ (分别地, $P(e_0,d_1)$) 为对应的点 (分别地, 周期), 则可以作如下的比较:

$$[P(d_0,d_1):P(d_0,d_1')]\sim[\mathcal{P}(d_0)\mathcal{L}(d_1):\mathcal{P}(d_0)\mathcal{L}(d_1')]=[\mathcal{L}(e_0)\mathcal{L}(d_1):\mathcal{L}(e_0)\mathcal{L}(d_1')]\sim[P(e_0,d_1):P(e_0,d_1')],$$

也就是说, 我们通过周期的比较, 可以得到 Heegner 点的比较.

给定整数 $n\equiv 5,6,7 \pmod 8$, 令 $f:X_{\widehat{R}^\times}\to E$ 为 E 的关于在 $K_n=\mathbb{Q}(\sqrt{-n})$ 上的平凡特征的本原模参数化, 则有

$$\sum_\chi P_\chi(f)=2^kQ_n,\quad Q_n:=\mathrm{Tr}_{H_{K_n}/H_0}P,$$

这里 $\chi=\chi_{d_0,d_1}$ 跑遍 K 的所有的亏格特征. 回顾 (4.1) 将 $P_\chi(f)$ 与 $\mathcal{P}(d_0)\mathcal{L}(d_1)$ 联系起来. 我们可以通过归纳法将 $\mathcal{P}(n)$ 表示为亏格点 Q_d (其中 $d\equiv 5,6,7 \pmod 8$) 和 $\mathcal{L}(d)$ (其中 $d\equiv 1,2,3 \pmod 8$) 的组合. 它们的 2 进非平凡性与亏格类数 $g(d)$ 相关, 正像我们之前所举例的 Heegner-Birch 方法一样. 这里的亏格类数 $g(d)$ 定义为 $2\mathcal{C}_d$ 的大小, 其中 $\mathcal{C}_d$ 是 $K_d=\mathbb{Q}(\sqrt{-d})$ 的理想类群. 注意到 $g(d)$ 是奇数当且仅当 K_d 没有阶数为 4 的理想类. 根据 Gauss 的亏格理论, 容易找出 $g(d)$ 的奇偶性.

下面是我们的主要结果:

定理 4.2 [16] 当 $n\equiv 5,6,7 \pmod 8$ 时, $\mathcal{L}(n)$ 是一个整数. 对于 $n\equiv 5,7 \pmod 8$, $2^{-\rho(n)}\mathcal{L}(n)$ 是

奇数, 如果

$$\sum_{\substack{n=d_0\cdots d_\ell\\ d_i\equiv 1 \pmod 8,\ i>0}} \prod_i g(d_i)\equiv 1 \pmod 2, \quad 或 \quad \sum_{\substack{n=d_0\cdots d_\ell,\\ d_0\equiv 5,7 \pmod 8\\ d_1\equiv 2,3 \pmod 8\\ d_i\equiv 1 \pmod 8,\ i>1}} \prod_i g(d_i)\equiv 1 \pmod 2.$$

对于 $n\equiv 6 \pmod 8$, $2^{-\rho(n)}\mathcal{L}(n)$ 是奇数, 如果

$$\sum_{\substack{n=d_0\cdots d_\ell,\\ d_0\equiv 5,6,7 \pmod 8\\ d_1\equiv 2,3 \pmod 8\\ d_i\equiv 1 \pmod 8,\ i>1}} \prod_i g(d_i)\equiv 1 \pmod 2.$$

这里所有的分解 $n=d_0\cdots d_\ell$ 都是不计顺序的, 并且满足 $d_i>1$ 对任意 i 成立.

上面定理中出现的 $\rho(n)$ 是一个整数, 满足 $0\leqslant\rho(n)\leqslant \mathrm{rank}_{\mathbb{Z}} E^{(n)}(\mathbb{Q})$, 并按照如下的方式定义. 令 $A=(X_0(32),\infty): 2v^2=u^3+u$, $A_n: 2nv^2=u^3+u$. 令 $\varphi_n: A_n\to E^{(n)}$ 为一个次数为 2 的同源, 定义 $\rho(n)$ 为非负整数使得 $2^{\rho(n)}=[E^{(n)}(\mathbb{Q}):\varphi_n(A_n(\mathbb{Q}))+E^{(n)}[2]]$.

令 $s(n)$ 为 $E^{(n)}: ny^2=x^3-x$ 的 2-Selmer 群模掉 $E^{(n)}[2]$ 所得到的 $\mathbb{F}_2$- 线性空间的维数, 则

$$s(n)=\mathrm{rank}\, E^{(n)}(\mathbb{Q})+\dim_{\mathbb{F}_2} Ш(E^{(n)}/\mathbb{Q})[2].$$

定理 4.3 [25,26] 令 Σ 为所有无平方因子的模 8 余 5 (分别地, 模 8 余 6 或 7) 的正整数 n 的全体, 则其中满足 $s(n)=1$ 的整数全体构成的子集 $\Sigma_1\subset\Sigma$ 的密度是

$$2\prod_{k=1}^{\infty}(1+2^{-k})^{-1}=0.8388\cdots.$$

定理 4.4 [14] 令 Σ_1 为所有无平方因子的模 8 余 5 (分别地, 模 8 余 6 或 7) 并满足 $s(n)=1$ 的正整数 n 的全体, 令 Σ_1' 为所有无平方因子的模 8 余 5 (分别地, 模 8 余 6 或 7) 并满足定理 4.2 中的充分条件的正整数 n 的全体, 则 Σ_1' 是 Σ_1 的子集, 密度为 $\frac{3}{4}$ (分别地, $\frac{1}{2}$ 或 $\frac{3}{4}$).

结合定理 4.2–4.4, 得到主定理 A(i). 类似地, 可以证明关于非同余数的 (ii).

5 精确 BSD 猜想

当无平方因子的正整数 n 满足主定理 B 中的条件时, $E^{(n)}: ny^2=x^3-x$ 在一个大于等于 3 的素数 p 处的约化情形只可能有以下三种:

(1) 好的通常约化;

(2) 好的超奇异约化;

(3) 潜在好的通常约化,

而不会出现潜在好的超奇异约化. 我们在第 6 节将看到, $E^{(n)}$ 的解析秩为 1. 在这个前提下, 对于前两种情形, BSD 公式的 p 部分分别由 Perrin-Riou [20] 和 Kobayashi [21] 证明. 在潜在好的通常约化情形, 我们有如下结果:

定理 5.1 2) 设 $E/\mathbb{Q}$ 是带复乘的椭圆曲线, K 是它的复乘域. 令 p 为一个在 K 中分裂的奇素数.

2) Li Y, Liu Y, Tian Y. On the Birch and Swinnerton-Dyer conjecture for rank one CM modular forms. Preprint

(i) 假设 $L(E,s)$ 在 $s=1$ 有一个单零点, 则 $E(\mathbb{Q})$ 的秩为 1, $Ш(E/\mathbb{Q})$ 是有限群, 并且关于 E 的 BSD 公式的 p 部分成立.

(ii) 如果 $E(\mathbb{Q})$ 的秩为 1, 并且 $Ш(E/\mathbb{Q})[p^\infty]$ 是有限群, 则 $L(E,s)$ 在 $s=1$ 有一个单零点.

注 5.2 定理 5.1(i) 的前半部分是 Gross 和 Zagier [9] 及 Kolyvagin [10] 的结果. 当 p 是好的通常约化的素数时, 后半部分是 Perrin-Riou [20] 的结果. 因此, 定理 5.1 所做的是 $p\geqslant 3$ 是坏的潜在通常约化素数的情形.

为了主定理 B 证明的完备性, 以下简要陈述定理 5.1 的证明. 证明的两个主要成分是 Rubin 的双变元 Iwasawa 主猜想和 p 进 Gross-Zagier 公式. 由于 $L(s,E)$ 在 $s=1$ 处有单零点, 我们可以选取好的辅助的虚二次域 $\mathcal{K}$ 使得 p 在 $\mathcal{K}$ 中分裂并且 $L(s,E/\mathcal{K})$ 在 $s=1$ 处仍然只有简单零点. 记 $\eta:\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})\to\{\pm1\}$ 为对应于二次扩张 $\mathcal{K}/\mathbb{Q}$ 的二次特征, η_K 为 η 在 $\mathrm{Gal}(\overline{\mathbb{Q}}/K)$ 上的限制. 令 $\mathbb{Q}_\infty$ 为 $\mathbb{Q}$ 的 $\mathbb{Z}_p$- 扩张, $\Gamma=\mathrm{Gal}(\mathbb{Q}_\infty/\mathbb{Q})$. 对 Γ 的任意有限特征 ν, 令 ν_K 为它在 $\mathrm{Gal}(K\mathbb{Q}_\infty/K)$ 上的限制, 那么下述等式对于定理 5.1 有至关重要的作用:

$$L(s,E\otimes\nu)L(s,E^{(\mathcal{K})}\otimes\nu)=L(s,E_{\mathcal{K}}\otimes\nu_{\mathcal{K}}). \tag{5.1}$$

考虑这个等式在 $s=1$ 处的特殊值, 那么等式左端插值了 Katz 的双变元的 p 进 L 函数, 右端插值了 p 进 Rankin-Selberg L 函数. 证明分为如下三个步骤:

(1) Rubin 的双变元 Iwasawa 主猜想 [19] 把 $Ш(E/K)$ 的 p 部分的阶与 Katz 的 p 进 L 函数的导数相联系. 此处需要注意, 对奇素数 p, 有 $\mathrm{ord}_p(|Ш(E/K)|)=2\mathrm{ord}_p(|Ш(E/\mathbb{Q})|)$.

(2) 复 Gross-Zagier 公式和 p 进 Gross-Zagier 公式将 Rankin-Selberg L 函数的导数、p 进 Rankin-Selberg L 函数的导数和 Heegner 点相联系.

(3) (5.1) 和插值公式可以推导出 Katz p 进 L 函数的导数与 Rankin-Selberg L 函数的导数的精确关系.

以下对它们作稍微更详细的介绍.

记 $p\mathcal{O}_K=\mathfrak{p}\bar{\mathfrak{p}}$. 需要固定 $\bar{\mathbb{Q}}\to\bar{\mathbb{Q}}_p$ 的嵌入, 设在这个嵌入之下, $K_{\mathfrak{p}}=\mathbb{Q}_p$. 令 φ 为 E 所对应的 Hecke 特征, 以及 $\mathfrak{f}$ 为 φ 的导子. 令 $\mathfrak{f}^{(p)}$ 为 $\mathfrak{f}$ 与 p 互素的部分.

定理 5.3 (双变元 p 进 L 函数 [27]) 令 $\mathfrak{g}$ 为任意一个与 p 互素的 K 的整理想, 满足 $\mathfrak{f}^{(p)}\mid\mathfrak{g}$. 在 $G=\mathrm{Gal}(K(\mathfrak{g}p^\infty)/K)$ 上存在唯一测度 $\mu_{\varphi,\mathfrak{g}}$ 使得对任意 G 的有限阶特征 χ, 有

$$\chi(\mu_{\varphi,\mathfrak{g}}):=\int_G\chi d\mu_{\varphi,\mathfrak{g}}=\frac{\tau(\chi_{\mathfrak{p}}\varphi_{\mathfrak{p}},\psi_{\mathfrak{p}})}{\tau(\varphi_{\mathfrak{p}},\psi_{\mathfrak{p}})}\frac{1-\chi\varphi(\mathfrak{p})p^{-1}}{1-\overline{\chi\varphi}(\mathfrak{p})p^{-1}}\frac{L^{(\mathfrak{g}p)}(\chi\varphi,1)}{\Omega_E},$$

这里 $K(\mathfrak{g}p^\infty)$ 是 K 的导子为 $\mathfrak{g}p^\infty$ 的类域, $L^{(\mathfrak{g}p)}(\chi\varphi,s)$ 是 $\chi\varphi$ 的整除 $\mathfrak{g}p$ 的素点处的 Euler 因子移除之后的非本原 L 函数.

注 5.4 众所周知, 我们可将 $\mu_{\varphi,\mathfrak{g}}$ 典范地等同于 Iwasawa 代数 $\widehat{\mathbb{Z}_p^{ur}}[[G]]$ 中的元素, $\widehat{\mathbb{Z}_p^{ur}}$ 为 $\mathbb{Z}_p$ 的极大非分歧扩张的完备化.

注 5.5 令 $G'=\mathrm{Gal}(K(\mathfrak{g}p^\infty)/\mathbb{Q})$, 则 G 是 G' 的一个指数为 2 的子群. 如果 χ' 是 G' 的一个特征使得 $\chi=\chi'|_G$ 成立, 则有

$$L(\chi\varphi,s)=L(E\otimes\chi',s).$$

特别地, 若 $\chi'=\eta_{\mathcal{K}}$ 是一个二次域 $\mathcal{K}\subset K(\mathfrak{g}p^\infty)$ 所对应的二次特征, 则有 $L(\chi\varphi,s)=L(E',s)$, 其中 $E'/\mathbb{Q}$ 是 E 的关于 $\mathcal{K}$ 的二次扭曲.

令 $\chi_{\mathrm{cyc}}:\mathrm{Gal}(\overline{K}/K)\to\mathrm{Gal}(K(\mu_{p^\infty})/K)\to\mathbb{Z}_p^\times$ 是 K 上的 p 进分圆特征, 由 Galois 群在所有 p 的指数次幂单位根上的作用给出. 由于对任意的整理想 $\mathfrak{g}$, $K(\mathfrak{g}p^\infty)\supset K(\mu_{p^\infty})$, 我们将它视作 G 上的特征.

定义 5.6 定义分圆方向的 p 进 L 函数为

$$\mathscr{L}_\varphi:\mathbb{Z}_p\to\mathbb{C}_p,\quad s\mapsto\chi_{\mathrm{cyc}}^{1-s}(\mu_{\varphi,\mathfrak{f}}).$$

根据复乘理论, 存在 K 的一个有限 Abel 扩张 F 和椭圆曲线 K 上带复乘的椭圆曲线 A, 使得

$$E\times_K F\simeq A\times_K F.$$

令 $F_\infty:=F(E[p^\infty]),F_0=F(E[p])$, 令 $\Gamma=\mathrm{Gal}(F_\infty/F_0)$, M_∞/F_∞ 为 F_∞ 的极大的在 $\mathfrak{p}$ 之外非分歧的 p- 扩张, 以及 $X_\infty:=\mathrm{Gal}(M_\infty/F_\infty)$, 那么, X_∞ 是有限生成的 $\mathbb{Z}_p[[\mathrm{Gal}(F_\infty/K)]]$- 模. 令 $\chi_0:\mathrm{Gal}(F_0/K)\to\mathcal{O}_{\mathfrak{p}}^\times$ 为在 $E[p]$ 上作用所诱导的特征, 那么, $X_\infty^{\chi_0}$ 是有限生成的 $\mathbb{Z}_p[[\Gamma]]$- 模. 记 $\mathrm{char}(X_\infty^{\chi_0})\in\mathbb{Z}_p[[\Gamma]]$ 为 $X_\infty^{\chi_0}$ 的特征理想; 另一方面, 需要注意到, $K(\mathfrak{f}p^\infty)\subset F_\infty$. 此时, 有下面的定理:

定理 5.7 (Rubin 的 Iwasawa 主猜想 [19]) 若 E/K 是带复乘 K 的椭圆曲线, 则

$$\mathrm{char}(X_\infty^{\chi_0})\cdot\widehat{\mathbb{Z}_p^{ur}}[[\Gamma]]=(\mu_{\mathfrak{f},\varphi}^{\chi_0}).$$

推论 5.8 设 E 是 K 上带复乘 K 的椭圆曲线, 令 $r=\mathrm{rank}_{\mathcal{O}_K}E(K)$. 假设 $Ш(E/K)[p^\infty]$ 有限, 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) E/K 的 p 进 BSD 猜想成立:

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

此处, 当 w_K 等于 4 或 6 时, 我们额外假设 E 在 $\mathfrak{p}$ 和 $\overline{\mathfrak{p}}$ 处同时有好约化或坏约化, $R_p(E/K)$ 是 $E(K)$ 关于其 p 进高度的正规子, $\mathscr{L}_\varphi^{(r)}$ (分别 $\mathscr{L}_{\overline{\varphi}}^{(r)}$) 表示对 $\mathscr{L}_\varphi$ (分别 $\mathscr{L}_{\overline{\varphi}}$) 作 r- 次求导.
进一步地, 当 E 定义在 $\mathbb{Q}$ 上时, 有

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

如果用符号 $\sim$ 表示在相差一个 p 进单位的意义下相等, 即它们的 p 进赋值相等, 那么, 上面的结论给出

$$\#Ш(E/K)[p^\infty]\sim\frac{\mathscr{L}_\varphi^{(r)}(1)\mathscr{L}_{\overline{\varphi}}^{(r)}(1)}{R_p(E(K))},\quad \#Ш(E/\mathbb{Q})[p^\infty]\sim\frac{\mathscr{L}_\varphi^{(r)}(1)}{R_p(E(\mathbb{Q}))}.\tag{5.2}$$

注 5.9 推论 5.8 是对定理 5.7 用 Schneider 的递降过程. 需要注意的是, Schneider 的递降过程只对在 p 之上的素点处有好约化的椭圆曲线有效, 而 E 并不满足这个条件. 因此, 事实上是对 A 应用递降过程, 并通过比较 A 和 E 的算术量来得到我们想要的结果2).

选取另一个辅助的二次域 $\mathcal{K}$ 满足如下条件:

(1) p 在 $\mathcal{K}$ 中分裂;

(2) $L(E_{\mathcal{K}}, s)$ 在 $s=1$ 处有一个单零点;

(3) $(E, \mathcal{K})$ 满足 Heegner 假设,

则有 Gross-Zagier 公式[9], 它将 $L'(E_{\mathcal{K}}, 1)$ 和 $h(P_{\mathcal{K}})$ 联系起来, 其中 $P_{\mathcal{K}}$ 是关于 $(E, \mathcal{K})$ 的 Heegner 点. 另一方面, 令 $G' = \mathrm{Gal}(\mathcal{K}_\infty/\mathcal{K})$, 其中 $K'_\infty/\mathcal{K}$ 是 $\mathbb{Z}_p^2$ 扩张, 则存在一个测度 $\mu_{\mathrm{RS}} \in \mathbb{Z}_p[[G']]$, 它插值了 Rankin-Selberg L 函数, 更确切地, 对任意 G' 的有限阶特征 χ', 有

$$\int_{G'} \chi' d\mu_{\mathrm{RS}} = \frac{L^{(p)}(1, E_{\mathcal{K}} \otimes \chi')}{8\pi^2(\phi, \phi)} \cdot \prod_{w|p} Z_w(\chi'_w, \psi_w),$$

其中 ϕ 是对应于 E 的新形式, (ϕ, ϕ) 是 ϕ 的 Peterson 范数:

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

$Z_w(\chi_w, \psi_w)$ 的定义参见脚注 2) 的第 3 节.

定义

$$\mathscr{L}_{\mathrm{RS}} : \mathbb{Z}_p \to \mathbb{C}_p, \quad s \mapsto \int_{G'} {\chi'}_{\mathrm{cyc}}^{1-s} d\mu_{\mathrm{RS}},$$

则有 p 进 Gross-Zagier 公式[20], 它将 $\mathscr{L}'_{\mathrm{RS}}(1)$ 和 $h_p(P_{\mathcal{K}})$ 联系起来. 事实上, 利用精确 Gross-Zagier 公式 (3.1) 和 p 进 Gross-Zagier 公式, 可得

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

因此,

$$\frac{L'(E_{\mathcal{K}}, 1)}{\Omega_{E/\mathcal{K}} h(P_{\mathcal{K}})} \sim \frac{\mathscr{L}'_{\mathrm{RS}}(1)}{h_p(P_{\mathcal{K}})}.$$

对任意 $\mathrm{Gal}(\mathbb{Q}_\infty/\mathbb{Q})$ 的有限阶特征 χ, 令 $\chi' = \chi\,|_{\mathrm{Gal}(\mathcal{K}\mathbb{Q}_\infty/\mathcal{K})}$, 则有

$$L(E \otimes \chi, s) L(E' \otimes \chi, s) = L(E/\mathcal{K} \otimes \chi', s),$$

其中 E' 是 E 关于 $\mathcal{K}$ 的二次扭曲. 特别地, 根据连续性, 用有限阶特征来逼近 $\chi_{\mathrm{cyc}}^{1-s}$, 由 p 进 L 函数的插值性质和上述等式可以得到

$$\mathscr{L}_\varphi(s) \mathscr{L}_{\varphi\eta_K}(s) = \mathscr{L}_{\mathrm{RS}}(E/\mathcal{K}, s) \cdot \frac{\Omega_E \Omega_{E'}}{\Omega_{E/\mathcal{K}}},$$

其中 η_K 是 $\mathcal{K}$ 所对应的二次特征 $\eta : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \{\pm 1\}$ 在子群 $\mathrm{Gal}(\overline{\mathbb{Q}}/K)$ 上的限制. 在 $s=1$ 处求导即得

$$\mathscr{L}'_\varphi(1) \mathscr{L}_{\varphi\eta_K}(1) = \mathscr{L}'_{\mathrm{RS}}(E/\mathcal{K}, 1) \frac{\Omega_E \Omega_{E'}}{\Omega_{E/\mathcal{K}}}.$$

对 E' 应用 (5.2), 得到

$$\#Ш(E'/\mathbb{Q})[p^\infty] \sim \frac{\mathscr{L}^{(r)}_{\varphi\eta_K}(1)}{R_p(E'(\mathbb{Q}))}. \tag{5.3}$$

于是,

$$\#Ш(E/\mathcal{K})[p^\infty] \sim \frac{\mathscr{L}'_\varphi(1) \mathscr{L}_{\varphi\eta_K}(1)}{R_p(E(\mathcal{K}))} \sim \frac{\mathscr{L}'_{\mathrm{RS}}(1)}{R_p(E(\mathcal{K}))}.$$

另一方面,

$$\frac{\mathscr{L}'_{\mathrm{RS}}(1)}{R_p(E(\mathcal{K}))}=\frac{\mathscr{L}'_{\mathrm{RS}}(1)[E(\mathcal{K}):\mathbb{Z}P_{\mathcal{K}}]^2}{h_p(P_{\mathcal{K}})}\sim\frac{L'(E/\mathcal{K},1)[E(\mathcal{K}):\mathbb{Z}P_{\mathcal{K}}]^2}{\Omega_{E/\mathcal{K}}h(P_{\mathcal{K}})}=\frac{L(E/\mathcal{K},1)}{\Omega_{E/\mathcal{K}}R(E(\mathcal{K}))}.$$

因此,

$$\#\text{Ш}(E/\mathcal{K})[p^\infty]\sim\frac{L(E/\mathcal{K},1)}{\Omega_{E/\mathcal{K}}R(E(\mathcal{K}))}.$$

将其与 (5.3) 结合, 就得到定理 5.1 中 BSD 公式的 p 部分的论断.

6 归纳方法与 Heegner 点非平凡性

本节引入对素因子个数研究周期和 Heegner 点的归纳法来证明它们的非平凡性. 特别地, 本节证明了主定理 B 中 BSD 猜想的秩部分及 BSD 公式的 2 部分.

定理 6.1 (参见定理 6.7 和 6.11) 令 $E: y^2=x^3-x$ 为同余椭圆曲线. 令 $n\equiv 5 \pmod 8$ 为一个无平方因子正整数, 其每个素因子都 $\equiv 1 \pmod 4$, 则能构造 E 上的 Heegner 点 $y_n\in E(\mathbb{Q}(\sqrt{n}))$ (其定义参见定理 6.7). 更进一步地, 若 $\mathbb{Q}(\sqrt{-n})$ 不存在阶数恰好为 4 的理想类, 则 $y_n\notin 2^{k-1}E(\mathbb{Q}(\sqrt{n}))^-+E[2]$, 其中 k 为 n 的素因子个数. 特别地, y_n 是一个无限阶点, n 是一个同余数, $E^{(n)}: ny^2=x^3-x$ 的 L 函数在 $s=1$ 处有单零点, 且还有 $E^{(n)}$ 的 BSD 公式的 2 部分成立.

在上述定理中, $E(\mathbb{Q}(\sqrt{n}))^-$ 是 $E(\mathbb{Q}(\sqrt{n}))$ 中那些在 Galois 群 $\mathrm{Gal}(\mathbb{Q}(\sqrt{n})/\mathbb{Q})$ 中的非平凡元作用下变为负的元素的集合, 且有 $E(\mathbb{Q}(\sqrt{n}))^-\cong E^{(n)}(\mathbb{Q})$ (我们在定理 2.1 的证明中已经使用过该记号).

注 6.2 对满足定理中的 n, 容易计算 $E^{(n)}$ 的 2-Selmer 群模掉 $E^{(n)}[2]$ 的 $\mathbb{F}_2$ 维数是 1, 由上述定理及 Kolyvagin 定理[10] 知, $\text{Ш}(E^{(n)})$ 的 2 部分平凡. 再由 Gross-Zagier 公式 (定理 6.3), 从 y_n 的 2-可除性可知, $\text{Ш}_{\mathrm{an}}(E^{(n)})$ 是一个奇数. 这样 BSD 公式的 2 部分由上面定理中 Heegner 点的 2- 可除性得到.

在本节中, 令 $E: y^2=x^3-x$, 对任意整数 n, 有 $E^{(n)}: ny^2=x^3-x$.

6.1 相关 Heegner 点的构造

我们将在模曲线上造点并通过模参数化态射投射到 E 上. 为方便起见, 先引入模曲线的一些记号. 对任意 $\mathrm{GL}_2(\widehat{\mathbb{Q}})$ 的开紧子群 U, 记 X_U 是级为 U 的定义在 $\mathbb{Q}$ 上的模曲线. X_U 的复点如下构成一个 Riemann 曲面:

$$X_U(\mathbb{C})=\mathrm{GL}_2(\mathbb{Q})_+\backslash(\mathcal{H}\cup\mathbb{P}^1(\mathbb{Q}))\times\mathrm{GL}_2(\widehat{\mathbb{Q}})/U.$$

对任意 $z\in\mathcal{H}\cup\mathbb{P}^1(\mathbb{Q})$ 和 $g\in\mathrm{GL}_2(\widehat{\mathbb{Q}})$, 记 $[z,g]_U$ 为 $X_U(\mathbb{C})$ 在上述复单值化下对应于 (z,g) 的点, 并记 $[z]_U=[z,1]_U$.

首先考虑模曲线 $X_0(32)=X_{U_0(32)}$, 其中 $U_0(32)\subset\mathrm{GL}_2(\widehat{\mathbb{Z}})$ 是一个紧开子群, 包含了满足 $c\equiv 0 \pmod{32}$ 的矩阵 $\left(\begin{smallmatrix}a&b\\c&d\end{smallmatrix}\right)$. 我们知道, $A:=(X_0(32),[\infty])$ 是一个 $\mathbb{Q}$ 上的椭圆曲线 (参见文献 [16, 第 742 页]), 带复乘 $\mathbb{Z}[\mathrm{i}]$, 并且

$$\mathrm{Aut}_{\mathbb{Q}(\mathrm{i})}(X_0(32)_{\mathbb{Q}(\mathrm{i})})\cong A(\mathbb{Q}(\mathrm{i}))\rtimes\mathrm{Aut}(A_{\mathbb{Q}(\mathrm{i})})\cong\mathbb{Z}[\mathrm{i}]/(1+\mathrm{i})^3\rtimes\mu_4.$$

令 E 为同余椭圆曲线 $y^2=x^3-x$. 令 $f_0: X_0(32)\to E$ 为一个定义在 $\mathbb{Q}$ 上的次数为 2 的同源, 将 $[\infty]$ 映成 O.

下面的结论是精确 Gross-Zagier 公式 (定理 3.1) 的一个推论:

定理 6.3 令 $n \equiv 5 \pmod 8$ 为一个无平方因子的正整数. 令 $K = \mathbb{Q}(\sqrt{-n})$ 以及 χ 为 K 上的一个非分歧二次特征, 使得 $L(s, E, \chi)$ 的符号是 -1. 令 d_1 和 d_2 为两个无平方因子正整数, 使得 $L(s, E_K, \chi) = L(s, E^{(d_1)})L(s, E^{(d_2)})$. 按

$$\sqrt{-n} \mapsto \begin{pmatrix} -1 & 1/4 \\ -4(n+1) & 1 \end{pmatrix}$$

定义一个 $\mathbb{Q}$- 嵌入 $K \to M_2(\mathbb{Q})$, 并按如下方式定义一个点 $P \in X_0(32)$. 令 $P_0 = [h, 1]_{U_0(32)} \in X_0(32)$, 其中 $h \in \mathcal{H}$ 为唯一的被 $K^\times$ 所固定的点, 并令 $P = (1 \pm [\mathrm{i}])P_0$, 若 $\chi_2(\varpi_2) = \mp 1$ (这里 χ_2 是 χ 的 2 部分, ϖ_2 是 K_2 的任意归一化子). 令 $f_0 : X_0(32) \to E$ 为前面所述的次数为 2 的模参数化, 则 $f_0(P)$ 在 $E(\overline{\mathbb{Q}})/E(\overline{\mathbb{Q}})_{\mathrm{tor}}$ 中的等价类是定义在 K 的 Hilbert 类域 H 上的, 并且有

$$\widehat{h}\Big(\sum_{t \in \widehat{K}^\times / K^\times \widehat{\mathcal{O}}_K^\times} f_0(P)^{\sigma_t} \chi(t)\Big) = 2^4 \cdot \frac{L'(1, E, \chi)}{\Omega_\infty^{(d_1)} \Omega_\infty^{(d_2)}},$$

其中 $\widehat{h} : E(\overline{\mathbb{Q}}) \to \mathbb{R}$ 是 $\mathbb{Q}$ 上的 Néron-Tate 高度, $\Omega_\infty^{(n)}$ 为 $E^{(n)}$ 的 Néron 微分的实周期.

下面还将考虑另一条级比 $U_0(32)$ 更小的模曲线. 令 U 是 $U_0(32)$ 的指数为 2 的开子群, 它被如下的形式所定义: U 在 2 处的分量 U_2 包含了行列式在 $1 + 4\mathbb{Z}_2$ 中的矩阵, 则 X_U 作为一个 $\mathbb{Q}$ 上的概型与 $X_0(32)_{\mathbb{Q}(\mathrm{i})}$ 相等, 而且

$$\mathrm{Aut}_{\mathbb{Q}}(X_U) = \mathrm{Aut}_{\mathbb{Q}(\mathrm{i})}(X_0(32)_{\mathbb{Q}(\mathrm{i})}) \rtimes \{1, \epsilon\} \simeq \mathbb{Z}[\mathrm{i}]/(1+\mathrm{i})^3 \rtimes \mu_4 \rtimes \{1, \epsilon\},$$

其中 X_U 上的对合 $P \mapsto P^\epsilon$ 是通过关于 $\epsilon := \left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$ 的右平移给出的 (参见文献 [16, 第 737 页]).

定义 6.4 令 $n \equiv 5 \pmod 8$ 为一个正整数, $K = \mathbb{Q}(\sqrt{-n})$. 按照定理 6.3 中的方式固定一个 K 到 $M_2(\mathbb{Q})$ 的嵌入, 令 $h \in \mathcal{H}$ 为唯一的被 $K^\times$ 所固定的点. 令 $P := [h, 1]_U$ 为 X_U 上所对应的点. 记 $f : X_U \to E$ 为上述态射 $f_0 : X_0(32) \to E$ 和自然态射 $X_U \to X_0(32)$ 的复合. 定义点 z 如下:

$$z := (f + f \circ [\mathrm{i}])(P) = f((1 + [\mathrm{i}])P) \in E(\overline{\mathbb{Q}}).$$

对任意 K 上的非分歧二次特征 χ, 它对应于 K 的一个二次扩张 $K(\sqrt{d})$, 定义 Heegner 点

$$y_\chi = \mathrm{Tr}_{H/K(\sqrt{d})} z \in E(K(\sqrt{d})).$$

复乘理论告诉我们, $K(P) \subset K^{\mathrm{ab}}$, 而且 Galois 群

$$\mathrm{Gal}(K(P)/\mathbb{Q}) \xrightarrow{\sim} (\widehat{K}^\times / K^\times \mathbb{Z}_2(1 + 4\mathcal{O}_2)\widehat{\mathcal{O}}_K^{\times(2)}) \rtimes \{1, w\},$$

其中 w 在 $\widehat{K}^\times$ 上共轭作用. 点 P 在该群下的作用通过 Hecke 算子给出. 我们用 σ 表示上面同构的逆映射.

定理 6.5 设 $n \equiv 5 \pmod 8$, $K = \mathbb{Q}(\sqrt{-n})$. 对任意 $t \in \widehat{K}^\times$, 记 $z_t := z^{\sigma_t}$ 为 z 被 σ_t 所作用得到的点, 其中 z 是定义 6.4 中的点, 则

(1) 点 z_t 可以定义在 K 的 Hilbert 类域 H 上;

(2) $z_{\varpi t} + z_t = (0, 0)$, 其中 $\varpi = \sqrt{-n} - 1 \in K_2^\times$;

(3) 点 z_t 的复共轭 $\overline{z}_t$ 等于 $z_{t^{-1}}$.

对于任何一个 U 在 $\mathrm{GL}_2(\widehat{\mathbb{Q}})$ 中的正规化子 g, Hecke 作用 T_g 给出了 $\mathrm{Aut}_{\mathbb{Q}}(X_U)$ 中的一个元素. 特别地, 在复参数化下, T_g 将点 $[z,h]_U$ 映到 $[z,hg]_U$. 称 $\mathrm{Aut}_{\mathbb{Q}}(X_U)$ 中这样的元素为 X_U 上的一个模自同态 (modular automorphism). 定理 6.5 基于如下对 X_U 上模自同态的讨论.

命题 6.6 令 $n\equiv 5 \pmod 8$ 为一个正整数, $K=\mathbb{Q}(\sqrt{-n})$. 按照定理 6.3 中的方式固定一个 K 到 $M_2(\mathbb{Q})$ 的嵌入, 则其诱导了嵌入 $K^\times\to \mathrm{GL}_{2,\mathbb{Q}}$, 于是, $(\widehat{\mathbb{Z}}+4\widehat{\mathcal{O}}_K)^\times\subset U$. 更进一步地,

(1) $K_2^\times$ 正规化 U_2, 因此, 其在 X_U 上有一个作用, 也就是说, 存在一个自然映射 $K_2^\times/\mathbb{Q}_2^\times(1+4\mathcal{O}_2)\to \mathrm{Aut}_{\mathbb{Q}}(X_U)$. 群 $K_2^\times/\mathbb{Q}_2^\times(1+4\mathcal{O}_2)$ 的阶数是 8, 其由一个 4 阶元 $\varpi=\sqrt{-n}-1$ 和一个 2 阶元 $1+2\varpi$ 生成. 对任意 $Q\in X_U$, 有

$$Q^{\varpi\epsilon}=[-\mathrm{i}]Q+\tau(1);\quad Q^{1+2\varpi}=Q+\tau(2).$$

(2) 元素 $w=\left(\begin{smallmatrix}1&0\\8&-1\end{smallmatrix}\right)=w^{-1}\in \mathrm{GL}_2(\mathbb{Q})$ 正规化 $K^\times$, 并且对任意 $x\in K^\times$, 有 $wx=\overline{x}w$. 它也正规化 U, 其诱导的在 X_U 上的作用按照如下方式给出: 对任意 $Q\in X_U$, 有

$$Q^{w\epsilon}=[\mathrm{i}]Q+\tau(1-\mathrm{i}).$$

证明 记 $\mathcal{S}\subset X_0(32)$ 为其尖点全体构成的集合. 我们有 $\mathcal{S}=A[(1+\mathrm{i})^3]$ (参见文献 [15, 第 124 页]). 令

$$\tau:\mathbb{Z}[\mathrm{i}]/(1+\mathrm{i})^3\to\mathcal{S}$$

为一个唯一的同构, 使得 $\tau(0)=[\infty]$, $\tau(1)=[0]$, 则有

$$\tau(-1)=\left[\frac{1}{2}\right],\quad \tau(2)=\left[\frac{1}{16}\right],\quad \tau(\pm\mathrm{i})=\left[\pm\frac{1}{4}\right],\quad \tau(1\pm\mathrm{i})=\left[\pm\frac{1}{8}\right].$$

设 $g\in \mathrm{GL}_2(\widehat{\mathbb{Q}})$ 是一个元素, 则其在 X_U 上的左平移作用交换 X_U 的两个分支当且仅当 g 在复合映射

$$\mathrm{GL}_2(\widehat{\mathbb{Q}})\overset{\det}{\to}\widehat{\mathbb{Q}}^\times=\mathbb{Q}_+^\times\cdot\widehat{\mathbb{Z}}^\times\to(\mathbb{Z}_2/4\mathbb{Z}_2)^\times\cong\{\pm1\}$$

下的像是 -1. 例如, $\epsilon=\left(\begin{smallmatrix}1&0\\0&-1\end{smallmatrix}\right), w=\left(\begin{smallmatrix}1&0\\8&-1\end{smallmatrix}\right)$ 和 $\varpi=\left(\begin{smallmatrix}-2&1/4\\-4(n+1)&0\end{smallmatrix}\right)$ 都是这样的元素, 而 $1+2\varpi$ 不是. 因此, $\varpi\epsilon$、$1+2\varpi$ 和 $w\epsilon$ 所对应的 Hecke 算子为

$$Q^{\varpi\epsilon}=\alpha Q+R,\quad Q^{1+2\varpi}=\beta Q+S,\quad Q^{w\epsilon}=\gamma Q+T,$$

其中 $\alpha,\beta,\gamma\in\mu_4$, 而 $R,S,T\in\mathcal{S}$ 为尖点. 这些算子都属于 $\mathrm{Aut}_{\mathbb{Q}(\mathrm{i})}(X_0(32)_{\mathbb{Q}(\mathrm{i})})=\mathrm{Aut}(X_U/\mathbb{Q}(\mathrm{i}))\subset \mathrm{Aut}_{\mathbb{Q}}(X_U)$. 为了计算 R、S 和 T, 取 $Q=[\infty]$. 根据复单值化, 有

$$\begin{aligned}\mathcal{S}(\mathbb{C})&=\mathrm{GL}_2(\mathbb{Q})_+\backslash\mathbb{P}^1(\mathbb{Q})\times\mathrm{GL}_2(\widehat{\mathbb{Q}})/U_0(32)=P(\mathbb{Q})_+\backslash\mathrm{GL}_2(\widehat{\mathbb{Q}})/U_0(32)\\&=P(\mathbb{Q})_+\backslash P(\widehat{\mathbb{Q}})\cdot\mathrm{GL}_2(\widehat{\mathbb{Z}})/U=N(\mathbb{Z}_2)\backslash\mathrm{GL}_2(\mathbb{Z}_2)/U_0(32)_2.\end{aligned}$$

在 $\mathrm{GL}_2(\mathbb{Q}_2)$ 中, 有如下分解:

$$\varpi\epsilon=\begin{pmatrix}1/4&0\\0&8\end{pmatrix}\begin{pmatrix}-8&-1\\1&0\end{pmatrix}\begin{pmatrix}-(n+1)/2&0\\4(n+3)&1\end{pmatrix},$$

$$1+2\varpi=\begin{pmatrix}1&1/2\\0&1\end{pmatrix}\begin{pmatrix}1&0\\-16&1\end{pmatrix}\begin{pmatrix}4n+1&0\\8(7n+1)&1\end{pmatrix}.$$

于是, $R=[0]=\tau(1)$, $S=[1/16]=\tau(2)$, $T=[-1/8]=\tau(1-\mathrm{i})$. 为了计算 α、β 和 γ, 只需要考虑在尖点 $[0]$ 上的作用, 该尖点被 $\left(\begin{smallmatrix}0&1\\-1&0\end{smallmatrix}\right)$ 表示. 我们有如下分解:

$$\begin{pmatrix}0&1\\-1&0\end{pmatrix}\varpi\epsilon=\begin{pmatrix}8&0\\0&1/4\end{pmatrix}\begin{pmatrix}1&0\\8&1\end{pmatrix}\begin{pmatrix}(n+1)/2&0\\-4(n+3)&-1\end{pmatrix},$$
$$\begin{pmatrix}0&1\\-1&0\end{pmatrix}(1+2\varpi)=\begin{pmatrix}2&-1\\0&1/2\end{pmatrix}\begin{pmatrix}7&-3\\-2&1\end{pmatrix}\begin{pmatrix}4n-17&3\\8(n-5)&7\end{pmatrix},$$
$$\begin{pmatrix}0&1\\-1&0\end{pmatrix}w\epsilon=\begin{pmatrix}8&1\\-1&0\end{pmatrix}.$$

因此, $[0]^{\varpi\epsilon}=[-1/8]=\tau(1-\mathrm{i})$, $[0]^{1+2\varpi}=[1/2]=\tau(-1)$, $[0]^{w\epsilon}=[0]=\tau(1)$. 由此得到

$$\tau(1+\mathrm{i})=\alpha\tau(1)+\tau(1),\quad \tau(-1)=\beta\tau(1)+\tau(2),\quad \tau(1)=\gamma\tau(1)+\tau(1-\mathrm{i}).$$

从中得出 $\alpha=-\mathrm{i}$, $\beta=1$ 和 $\gamma=i$. □

定理 6.5 的证明 注意到自然态射 $X_U\to X_0(32)$ 在 ϵ 作用下不变. 令 $P_0\in X_0(32)$ 为 P 在此自然态射下的像. 根据命题 6.6, 可得

(i) $P_0^{\sigma_\varpi}=[-\mathrm{i}]P_0+\tau(1)$;

(ii) $P_0^{\sigma_{1+2\varpi}}=P_0+\tau(2)$;

(iii) $\overline{P}_0=[\mathrm{i}]P_0+\tau(1-\mathrm{i})$.

令 $f_0:X_0(32)\to E$ 为前面提到的次数 2 的模参数化, 则 f_0 将 $\tau(1)$、$\tau(2)$ 和 $\tau(1\pm\mathrm{i})$ 分别映成 $(1,0)$、O 和 $(0,0)$. 容易看到由 (ii) 有 $z_1^{\sigma_{1+2\varpi}}=z_1$. 根据 (i), 有

$$z_1^{\sigma_\varpi}=f_0([1-\mathrm{i}]([-\mathrm{i}]P_0+\tau(1)))=f_0(-[1+\mathrm{i}]P_0+\tau(1-\mathrm{i}))=-z_1+(0,0),$$

因此, $z_1^{\sigma_{\varpi^2}}=z_1$, 进而, $z_1^{\sigma_{1+\varpi}}=z_1$. 于是, (1) 和 (2) 成立. 根据 (iii), 有

$$\overline{z}_t=\overline{f_0([1+\mathrm{i}]P_0)}^{\sigma_{t^{-1}}}=f_0([1-\mathrm{i}]([\mathrm{i}]P_0+\tau(1-\mathrm{i})))^{\sigma_{t^{-1}}}=f_0([1+\mathrm{i}]P_0)^{\sigma_{t^{-1}}}=z_{t^{-1}}.$$

证毕. □

6.2 Heegner 点的归纳方法

下面一个定理 (再加上 Kolyvagin 的定理) 说明主定理 B 中 BSD 猜想秩部分成立.

定理 6.7 令 $n\equiv 5 \pmod 8$ 为一个无平方因子正整数, 其每个素因子都 $\equiv 1 \pmod 4$. 令 $k\geqslant 1$ 为其素因子个数, 则点

$$y_n:=\mathrm{Tr}_{H/K(\sqrt{n})}z_1$$

是定义在 $\mathbb{Q}(\sqrt{n})$ 上的, 并且属于 $2^{k-2}E(\mathbb{Q}(\sqrt{n}))^-+E[2]$. 更进一步地, 若 $K=\mathbb{Q}(\sqrt{-n})$ 的理想类群 $\mathcal{A}$ 不包含阶数恰好为 4 的元素, 等价地, 若 $\#2\mathcal{A}$ 是奇数, 则有

$$y_n\notin 2^{k-1}E(\mathbb{Q}(\sqrt{n}))^-+E[2].$$

特别地, y_n 是一个无限阶点, 因此, n 是一个同余数.

先考虑定理 6.7 在 $k=1$ 时的情形, 即 $n=p\equiv 5 \pmod 8$ 是一个素数的情形. 定理 2.1 及其证明实际上给出了如下结论:

命题 6.8 令 $p\equiv 5 \pmod 8$ 为一个素数, 则点 y_p 满足 $y_p\in E(\mathbb{Q}(\sqrt{p})\setminus E(\mathbb{Q}(\sqrt{p}))^-$, 以及

$$2y_p\in E(\mathbb{Q}(\sqrt{p}))^-\setminus(2E(\mathbb{Q}(\sqrt{p}))^-+E[2]).$$

特别地, $2y_p$ 是无限阶点. 因此, p 是同余数.

以下考虑一般情形. 记 H_0 为 K 的 Hilbert 类域 H 的亏格域 (即 K 的极大的非分歧的指数为 2 的 Abel 扩张). 令 $\mathcal{A}=\widehat{K}^\times/K^\times\widehat{\mathcal{O}}_K^\times$ 为 K 的理想类群, 则在类域论给出的同构 $\mathcal{A}\cong \mathrm{Gal}(H/K)$ 下, 有 $2\mathcal{A}\cong \mathrm{Gal}(H/H_0)$.

定义 6.9 定义 $y_0=\mathrm{Tr}_{H/H_0}z\in E(H_0)$. 对每个 n 的正因子 d 满足 $d\equiv 5 \pmod 8$, 定义

$$y_d:=\mathrm{Tr}_{H/K(\sqrt{d})}z\in E(K(\sqrt{d})).$$

引理 6.10 设 $k\geqslant 2$, 则

(1) 对每个 n 的正因子 d 满足 $d\equiv 5 \pmod 8$, 有 $y_d\in E(\mathbb{Q}(\sqrt{d}))^-$;

(2) 我们有 $y_0\in E(H_0^+)$, 其中 $H_0^+=H_0\cap\mathbb{R}$, 并且其满足

$$y_0+y_0^{\sigma_\varpi}=\#2\mathcal{A}\cdot(0,0).$$

这些点还满足如下的关系:

$$\sum_{1\leqslant d\mid n, d\equiv 5 \pmod 8} y_d=\begin{cases}2^{k-1}y_0, & 若\ k\geqslant 3,\\ 2^{k-1}y_0+\#2\mathcal{A}\cdot(0,0), & 若\ k=2.\end{cases}$$

证明 对任意 $\sigma\neq 1,\sigma_\varpi$, 有

$$\begin{aligned}m_\sigma&:=\#\{d:\ 1\leqslant d\mid n, d\equiv 5 \pmod 8, \sigma\in \mathrm{Gal}(H_0/K(\sqrt{d}))\}\\&=\sum_{d\mid n}\frac{\chi_d(\sigma)+1}{2}\cdot\frac{1-\chi_d(\sigma_\varpi)}{2}=2^{k-2}.\end{aligned}$$

这里注意到, 对任意 n 的正因子 d, $\sigma_\varpi(\sqrt{d})=(\frac{2}{d})\sqrt{d}$. 于是,

$$\begin{aligned}\sum_{d\mid n,\equiv 5 \pmod 8} y_d-2^{k-1}y_0&=\sum_{d\mid n,\equiv 5 \pmod 8}(y_d-y_0)=\sum_{d\mid n,\equiv 5 \pmod 8}(y_d-y_0)\\&=\sum_{d\mid n,\equiv 5 \pmod 8}\ \sum_{1\neq\sigma\in \mathrm{Gal}(H_0/K(\sqrt{d}))} y_0^\sigma\\&=\sum_{1,\sigma_\varpi\neq\sigma\in \mathrm{Gal}(H_0/K)} m_\sigma y_0^\sigma=\sum_{1\neq\sigma,\sigma(\mathrm{i})=i}(m_\sigma y_0^\sigma+m_{\sigma\sigma_\varpi}y_0^{\sigma\sigma\varpi})\\&=2^{k-2}(2^{k-1}-1)\#2\mathcal{A}\cdot(0,0).\end{aligned}$$

这就完成了证明. □

定理 6.7 的证明 我们对 k 归纳. $k=1$ 时的情形由命题 6.8 给出. 接下来考虑 $k\geqslant 2$ 的情形. 根据引理 6.10, 有

$$y_n+\sum_{p_0\mid d\mid n, d\neq n} y_d=2^k y_0 \bmod E[2].$$

对每个固定的 $d \mid n$ 满足 $1 \leqslant d < n$, $d \equiv 5 \pmod 8$, 令 y_d^0 为与 y_d 的构造类似的点, 只不过将域 $K = \mathbb{Q}(\sqrt{-n})$ 替换成 $K_0 = \mathbb{Q}(\sqrt{-d})$. 令 χ 和 χ^0 为二次扩张 $\mathrm{Gal}(K(\sqrt{d})/K)$ 和 $\mathrm{Gal}(K_0(\sqrt{d})/K_0)$ 所对应的特征, 则 $2y_d$ 和 $2y_d^0$ 的高度由精确 Gross-Zagier 公式给出 (定理 6.3): 若 y_d^0 不是扭点, 则 y_d 与 y_d^0 在一维 $\mathbb{Q}$ 线性空间 $E(\mathbb{Q}(\sqrt{d}))^- \otimes_{\mathbb{Z}} \mathbb{Q}$ 上的比值是

$$[y_d : y_d^0]^2 = \frac{L^{\mathrm{alg}}(E^{(n/d)}, 1)}{L^{\mathrm{alg}}(E^{(1)}, 1)},$$

其中 L 函数特殊值的代数部分为

$$L^{\mathrm{alg}}(1, E^{(n/d)}) := \frac{L(1, E^{(n/d)})}{\Omega_\infty^{(n/d)}}.$$

根据定理 6.12, 它的 2 进赋值大于等于 $2(k_{n/d}+1)$. 根据归纳假设, 有 $y_d^0 \in 2^{k_d-2}E(\mathbb{Q}(\sqrt{d}))^- + E[2]$, 于是, $y_d \in 2^{k-1}E(\mathbb{Q}(\sqrt{d}))^- + E[2]$.

现在将 y_d 写为 $y_d = 2^{k-1}y_d' + t_d$, 其中 $y_d' \in E(\mathbb{Q}(\sqrt{d}))^-$, $t_d \in E[2]$, 则存在某个 $t \in E[2]$ 使得

$$y_n = 2^{k-1}\left(y_0 - \sum_{p_0 \mid d \mid n, d \neq n} y_d'\right) + t.$$

注意到 $H_0^+/\mathbb{Q}$ 的任意非平凡子扩张都要在某个奇素数处分歧, 于是,

$$E[2^\infty] \cap E(H_0^+) = E[2].$$

考虑 Kummer 映射

$$E(\mathbb{Q}(\sqrt{n}))/2^kE(\mathbb{Q}(\sqrt{n})) \hookrightarrow H^1(\mathbb{Q}(\sqrt{n}), E[2^k]),$$

以及扩充 - 限制 (inflation-restriction) 正合列

$$0 \to H^1(\mathrm{Gal}(H_0^+/\mathbb{Q}(\sqrt{n})), E[2]) \to H^1(\mathbb{Q}(\sqrt{n}), E[2^k]) \to H^1(H_0^+, E[2^k]).$$

由于 $2y_n = 2^k(y_0 - \sum_{p_0 \mid d \mid n, d \neq n} y_d')$, 其中 $y_0 - \sum_{p_0 \mid d \mid n, d \neq n} y_d' \in E(H_0^+)$, 我们知道 $2y_n$ 在 Kummer 映射下的像在 $H^1(\mathrm{Gal}(H_0^+/\mathbb{Q}(\sqrt{n})), E[2])$ 之中, 从而, 该像的 2 倍平凡. 因此, $4y_n \in 2^kE(\mathbb{Q}(\sqrt{n}))$, 或者等价地, 存在 $\widetilde{y}_n \in E(\mathbb{Q}(\sqrt{n}))$ 使得 $4(y_n - 2^{k-2}\widetilde{y}_n) = 0$. 因此, 在模掉 $E[2]$ 的意义下, 有 $y_n = 2^{k-2}\widetilde{y}_n$, 所以, $y_n \in 2^{k-2}E(\mathbb{Q}(\sqrt{n})) + E[2]$. 另一方面, 根据关系式

$$y_n = 2^{k-1}\left(y_0 - \sum_{d \equiv 5 \pmod 8, \neq n, d \mid n} y_d'\right) \bmod E[2],$$

有 $2^{k-2}(\widetilde{y}_n - 2y_0 + \sum_{d \neq n} 2y_d') \in E[2]$, 由此得出

$$\widetilde{y}_n = 2y_0 - \sum_{d \neq n} 2y_d' + t, \quad \text{对某个 } t \in E[2] \text{ 成立}.$$

对任意 $0 < d \mid n$ 满足 $p_0 \mid d$, 有 $\sigma_\varpi(\sqrt{d}) = -\sqrt{d}$, 于是, $(y_d')^{\sigma_\varpi} = -y_d'$. 因此, $\widetilde{y}_n^{\sigma_\varpi} + \widetilde{y}_n = 2(y_0^{\sigma_\varpi} + y_0) = 0$, 即 $\widetilde{y}_n \in E(\mathbb{Q}(\sqrt{n}))^-$. 这说明 $y_n \in 2^{k-2}E(\mathbb{Q}(\sqrt{n}))^- + E[2]$.

现在考虑 $\#2\mathcal{A}$ 是奇数的情形. 根据引理 6.10, 有 $y_0+y_0^{\sigma_\varpi}=(0,0)$. 假设 $y_n=2^{k-1}y_n'+t_n$ 对某个 $y_n'\in E(\mathbb{Q}(\sqrt{n}))^-$ 及 $t_n\in E[2]$ 成立, 则根据引理 6.10 中的关系式, 有

$$2^{k-1}\Big(y_0-\sum_{d|n,\equiv 5\ (\mathrm{mod}\ 8)} y_d'\Big)\in E[2].$$

由于 $H_0^+/\mathbb{Q}$ 的任意非平凡子扩张都要在某个奇素数处分歧, 因此有

$$t:=y_0-\sum_{d|n,\,d\equiv 5\ (\mathrm{mod}\ 8)} y_d'\in E(H_0^+)\cap E[2^{k+1}]=E[2].$$

于是得到

$$y_0+y_0^{\sigma_\varpi}=\sum_{d|n,\,d\equiv 5\ (\mathrm{mod}\ 8)}(y_d'+{y_d'}^{\sigma_\varpi})+(t+t^{\sigma_\varpi})=0,$$

这与 $y_0+y_0^{\sigma_\varpi}=(0,0)$ 矛盾, 因此假设不成立. □

由定理 6.7 可以得到下面一个定理, 它说明主定理 B 中 BSD 公式的 2 部分成立.

在证明过程中我们要用到一个 Abel 群上的 2 进赋值映射的概念. 设 A 是一个有限生成 Abel 群, 记 $\widehat{A}=A\otimes_{\mathbb{Z}}\mathbb{Z}_2$, 则定义 2 进赋值映射 $v:A\to\mathbb{Z}\cup\{\infty\}$ 如下: 若 $a\in A$ 是一个非扭元, 则定义 $v(a)$ 为最小的非负整数 v 使得 $a\in 2^v\widehat{A}+\widehat{A}[2^\infty]$, 但是 $a\notin 2^{v+1}\widehat{A}+\widehat{A}[2^\infty]$. 若 a 是一个扭元, 则定义 $v(a)=\infty$.

定理 6.11 令 $n\equiv 5\ (\mathrm{mod}\ 8)$ 为一个无平方因子的正整数, 其素因子分解为 $n=p_1\cdots p_k$ 并满足 $p_i\equiv 1\ (\mathrm{mod}\ 4)$. 假设 $\mathbb{Q}(\sqrt{-n})$ 不存在阶数恰好为 4 的理想类, 则有

$$\mathrm{rank}(E^{(n)}(\mathbb{Q}))=1=\mathrm{ord}_{s=1}L(s,E^{(n)}),$$

并且 $Ш(E^{(n)}/\mathbb{Q})$ 是一个阶数为奇数的有限群. 更进一步地, $E^{(n)}$ 的 BSD 公式的 2 部分成立.

证明 令

$$y:=\sum_{t\in\mathcal{A}} f(P)^{\sigma_t}\chi_n(t)\in E(\mathbb{Q}(\sqrt{n}))$$

为定理 6.3 中定义的 Heegner 点, 这里 χ_n 是对于二次扩张 $K(\sqrt{n})/K$ 的二次特征, 则定理 6.7 告诉我们, y 是一个无限阶点. 于是, 定理 6.3 中的 Gross-Zagier 公式告诉我们, $\mathrm{ord}_{s=1}L(s,E^{(n)})=1$. 根据 Kolyvagin [10] 的定理可知, $\mathrm{rank}\,E^{(n)}(\mathbb{Q})=1$ 以及 $Ш(E^{(n)}/\mathbb{Q})$ 是一个有限群. 根据 Monsky [25] 的计算, $Ш(E^{(n)}/\mathbb{Q})$ 的 2 部分是平凡的.

令 $v:E(\mathbb{Q}(\sqrt{n}))\to\mathbb{Z}\cup\{\infty\}$ 为 2 进赋值映射, 则可以根据定理 6.7 计算 $v(y)$, 并根据定理 6.3 计算 $\widehat{h}(y)$, 进而得到

$$v(y)=k-1,\quad \widehat{h}(y)=\frac{2L'(1,E^{(n)})}{\Omega_\infty^{(n)}}.$$

于是,

$$\widehat{h}(y)\cdot 2^{-2v(y)}=2^{-2k+3}\cdot\frac{L'(1,E^{(n)})}{\Omega_\infty^{(n)}}. \tag{6.1}$$

由于

$$\mathrm{rank}\,E^{(n)}(\mathbb{Q})=\mathrm{ord}_{s=1}L(E^{(n)},s)=1,$$

因此可以令 y^0 为秩为 1 的自由 Abel 群 $E^{(n)}(\mathbb{Q})/E^{(n)}(\mathbb{Q})_{\mathrm{tor}}$ 的一个生成元, 则 BSD 公式在此情形为

$$\frac{L'(1,E^{(n)})}{\Omega_\infty^{(n)}\cdot\widehat{h}(y^0)}=2^{-1}\cdot 4^{k-1}\#Ш(E^{(n)}/\mathbb{Q}),$$

等价地,

$$\widehat{h}(y^0)=2^{-2k+3}\cdot(\#Ш(E^{(n)}/\mathbb{Q}))^{-1}\cdot\frac{L'(1,E^{(n)})}{\Omega_\infty^{(n)}},$$

该式的 2 部分相等, 这根据的是 $Ш(E^{(n)}/\mathbb{Q})[2^\infty]$ 的平凡性, 以及前面关于 $\widehat{h}(y)2^{-2v(y)}$ 的等式 (6.1). □

6.3 周期的归纳法

在定理 6.7 的证明中, 我们需要关于 $L^{\mathrm{alg}}(E^{(n)},1)=L(E^{(n)},1)/\Omega_\infty^{(n)}$, $n\equiv 5 \pmod 8$ 的 2 进赋值的估计.

定理 6.12 令 $n=p_1\cdots p_k\equiv 1 \pmod 8$ 为两两不同的素数的乘积, 其中 $k\geqslant 1$, 则有

$$v(L^{\mathrm{alg}}(E^{(n)},1))\geqslant 2k-3.$$

如果更进一步地, 对任意 i 都有 $p_i\equiv 1 \pmod 4$, 则有 $v(L^{\mathrm{alg}}(E^{(n)},1))\geqslant 2k-1$.

我们将通过对周期作归纳, 利用 Waldspurger 公式对定理 6.12 给出一个类似定理 6.7 的证明.

令 B 是定义在 $\mathbb{Q}$ 上的恰好在 2 和 ∞ 处分歧的四元代数. 令 $\pi\subset C^\infty(B^\times\backslash B_{\mathbb{A}}^\times)$ 为 E 所对应的 $B_{\mathbb{A}}^\times$ 的自守表示. 可如下刻画 π: 对 $p\neq 2$, 局部表示 π_p 被 $B_p^\times$ 的极大紧子群固定住的子空间是一维的; Hecke 算子 T_p 在这个一维空间上的迹由 $a_p(E)$ 给出.

固定一个 $K:=\mathbb{Q}(\sqrt{-n})$ 到 B 的嵌入, 以及一个 B 的极大序模 $\mathcal{O}_B$ 使得 $\mathcal{O}_B\cap K=\mathcal{O}_K$. 令 $R=\mathcal{O}_K+4\mathcal{O}_B$, 则其为 B 的一个判别式为 32 的序模使得 $R\cap K=\mathcal{O}_K$. 令 $U=\widehat{R}^\times$, 则其为 $\widehat{B}^\times$ 的一个开子群并且存在一个自然映射 $\mathcal{A}\to B^\times\backslash\widehat{B}^\times/U$.

群 $K_2^\times/\mathbb{Q}_2^\times\mathcal{O}_{K,2}^\times$ 阶为 2, 记 $\chi_\pm$ 是它上面的两个特征. 记 $\pi_{\pm,\mathbb{Z}}^U$ 为 π 中被 U 固定的且在 $K_2^\times$ 是 $\chi_\pm$- 特征的整数值自守形式全体. 这是一个秩为 1 的自由 $\mathbb{Z}$ 模. 称其生成元为 $(E,K,\chi_\pm)$ 的本原测试向量.

令 $f_\pm$ 为一个 $(E,K,\chi_\pm)$ 的本原测试向量. 通过直接计算 (如文献 [16]) 可得下述结论:

命题 6.13 本原测试向量 $f_\pm$ 在 $2\mathcal{A}$ 上取值为奇.

取 $f'=f_++f_-$. 类比前一节秩为 1 时的情形, 我们给出如下定义.

定义 6.14 对 n 的每个正因子 d, 令 χ_d 为 K 的二次扩张 $K(\sqrt{d^*})\subset H_0$ 所对应的 $\mathcal{A}$ 的二次特征, 其中 $d^*=(-1)^{\frac{d-1}{2}}d$.

定义 $y_0=\sum_{t\in 2\mathcal{A}}f'(t)$, 对 n 的每个正因子 d, 定义 $y_d:=\sum_{t\in\mathcal{A}}f'(t)\chi_d(t)$.

容易看到如下关系成立:

$$\sum_{d|n}y_d=2^ky_0.$$

引理 6.15 我们有如下性质:

(1) 对 n 的任意正因子 d, 有

$$y_d=(-1)^{\frac{d^*-1}{4}}y_{n/d}.$$

(2) 若对任意 $p\mid n$, 有 $p\equiv\pm 1 \pmod 4$, 则 $2\mid y_0$.

这里, 若对任意 $p \mid n$, 都有 $p \equiv \pm 1 \pmod 4$, 则 $2\mathcal{A}$ 是偶数. 因而, 引理 6.15(2) 由命题 6.13 直接得到.

下面的结论是精确 Waldspurger 公式 (定理 3.2) 的一个推论.

定理 6.16 令 K 为一个虚二次域, χ 为一个 $\widehat{K}^\times/K^\times\widehat{\mathcal{O}}_K^\times$ 的二次特征, 使得 $L(s,E,\chi)$ 的符号是 $+1$. 固定一个嵌入 $\tau: K \to B$ 使得 $\mathcal{O}_B \cap K = \mathcal{O}_K$, 则有

$$\Big|\sum_{t\in\widehat{K}^\times/K^\times\widehat{\mathcal{O}}_K^\times} f'(t)\chi(t)\Big|^2 = 2^{2+a}\cdot u_K^2\cdot L^{\mathrm{alg}}(1,E,\chi),$$

其中 $u_K = [\mathcal{O}_K^\times : \mathbb{Z}^\times]$, $a=0$, 若 $8 \nmid D_K$; $a=1$, 在其余情形. 这里, 若 d_1 和 d_2 为两个正整数且满足 $L(s,E,\chi) = L(s,E^{(d_1)})L(s,E^{(d_2)})$, 则 $L^{\mathrm{alg}}(1,E,\chi) = L^{\mathrm{alg}}(E^{(d_1)},1)L^{\mathrm{alg}}(E^{(d_2)},1)$.

定理 6.12 的证明 根据引理 6.15, 有

(1) $y_d = 0$, 若 $d \equiv 5,7 \pmod 8$;

(2) $y_d + y_{n/d} = 0$, 若 $d \equiv 3 \pmod 8$;

(3) $y_d = y_{n/d}$, 若 $d \equiv 1 \pmod 8$.

于是,

$$2^k y_0 = \sum_{d\mid n} y_d = \sum_{d\mid n, d\equiv 1 \pmod 8} y_d. \tag{6.2}$$

现在对 k 归纳. 在 $k=1$ 的情形, $n = p \equiv 1 \pmod 8$ 是一个素数, 则有 $\#2\mathcal{A}$ 是偶数, 并且 $2 \mid y_0$. 于是,

$$|y_1|^2 = |y_p|^2 = 2^4 L^{\mathrm{alg}}(E^{(1)},1)L^{\mathrm{alg}}(E^{(p)},1).$$

另一方面, $y_1 + y_p = 4(y_0/2)$ 和 $y_1 = y_p$ 可以导出 $y_1 = 2(y_0/2)$. 因此, $v(L^{\mathrm{alg}}(E^{(p)},1)) \geqslant 1$ 而且等号成立当且仅当 $y_0/2$ 是奇数.

在 $k>1$ 的情形, 对任意 n 的模 8 余 1 的真因子 d, 有

$$|y_d|^2 = |y_{n/d}|^2 = 2^4 L^{\mathrm{alg}}(E^{(d)},1)L^{\mathrm{alg}}(E^{(n/d)},1).$$

根据上一个引理以及归纳假设知, $y_d = y_{n/d}$ 的 2 进赋值大于等于 $k-1$. 于是, $v(y_d + y_{n/d}) \geqslant k$. 根据 (6.2) 和 $y_1 = y_n$, 有 $v(y_1) \geqslant k-1$, 或者等价地, $v(L^{\mathrm{alg}}(E^{(n)},1)) \geqslant 2k-3$, 因为 $|y_1|^2 = 2L^{\mathrm{alg}}(E^{(n)},1)$.

在所有的因子 $p_i \equiv 1 \pmod 4$ 的情形, 有 $\#2\mathcal{A}$ 是偶数, 并且

$$\sum_{d\mid n, d\equiv 1 \pmod 8} y_d = 2^{k+1}\left(\frac{y_0}{2}\right).$$

于是, 当 $k=1$ 时, 我们所需的论断成立. 在 $k>1$ 的情形, 根据归纳假设可知, $v(y_d) = v(y_{n/d}) \geqslant k+1$, 于是, $v(y_d + y_{n/d}) \geqslant k+2$ (由于 $y_d = y_{n/d}$). 因此, $v(y_1) = v(y_n) \geqslant k$ 并且等号成立当且仅当 $y_0/2$ 是奇数. 于是得到 $v(L^{\mathrm{alg}}(E^{(n)},1)) \geqslant 2k-1$ 并且等号成立当且仅当 $2 \parallel y_0$. □

致谢 以此文恭贺杨乐先生八十寿辰, 感谢杨先生的长期支持和培养.

参考文献

1 Dickson L E. History of the Theory of Numbers, Volume II. New York: Chelsea, 1971

2 Mordell L J. On the rational solutions of the indeterminate equations of the third and fourth degrees. Proc Cambridge Philos Soc, 1922, 21: 179–182
3 Mazur B. Modular curves and the Eisenstein ideal. Publ Math Inst Hautes Études Sci, 1977, 47: 33–186
4 Lang S, Tate J. Principal homogeneous spaces over Abelian varieties. Amer J Math, 1958, 80: 659–684
5 Shafarevich I R. The group of principal homogeneous algebraic manifolds (in Russian). Dokl Akad Nauk SSSR, 1959, 124: 42–43
6 Silverman J H. The Arithmetic of Elliptic Curves, 2nd ed. New York: Springer, 2009
7 Birch B J, Swinnerton-Dyer H P. Notes on elliptic curves, II. J Reine Angew Math, 1965, 218: 79–108
8 Coates J, Wiles A. On the conjecture of Birch and Swinnerton-Dyer. Invent Math, 1977, 39: 223–251
9 Gross B H, Zagier D B. Heegner points and derivatives of L-series. Invent Math, 1986, 84: 225–320
10 Kolyvagin V A. Euler systems. In: The Grothendieck Festschrift, Volume II. Progress in Mathematics, vol. 87. Boston: Birkhäuser, 1990, 435–484
11 Goldfeld D. Conjectures on elliptic curves over quadratic fields. In: Number Theory. Lecture Notes in Mathematics, vol. 751. Berlin: Springer, 1979, 108–118
12 Katz N M, Sarnak P. Zeros of zeta functions and symmetry. Bull Amer Math Soc (NS), 1999, 36: 1–26
13 Birch B J, Stephens N M. The parity of the rank of the Mordell-Weil group. Topology, 1966, 5: 295–299
14 Smith A. 2^∞-Selmer groups, 2^∞-class groups, and Goldfeld's conjecture. ArXiv:1702.02325, 2017
15 Tian Y. Congruent numbers and Heegner points. Cambridge J Math, 2014, 2: 117–161
16 Tian Y, Yuan X, Zhang S W. Genus periods, genus points and congruent number problem. Asian J Math, 2017, 21: 721–774
17 Heegner K. Diophantische analysis und modulfunktionen. Math Z, 1952, 56: 227–253
18 Pan J. The p-adic BSD conjecture for elliptic curves over $\mathbb{Q}$ at potentially supersingular primes. PhD Thesis. Beijing: University of Chinese Academy of Sciences, 2017
19 Rubin K. The "main conjectures" of Iwasawa theory for imaginary quadratic fields. Invent Math, 1991, 103: 25–68
20 Perrin-Riou B. Points de Heegner et dérivées de fonctions L p-adiques. Invent Math, 1987, 89: 455–510
21 Kobayashi S. The p-adic Gross-Zagier formula for elliptic curves at supersingular primes. Invent Math, 2013, 191: 527–629
22 Cai L, Shu J, Tian Y. Explicit Gross-Zagier and Waldspurger formulae. Algebra Number Theory, 2014, 8: 2523–2572
23 Yuan X, Zhang S, Zhang W. The Gross-Zagier Formula on Shimura Curves. Princeton: Princeton University Press, 2012
24 Smith A. An approach to the full BSD conjecture at two in quadratic twist families of elliptic curves. Undergraduate Thesis. Princeton: Princeton University, 2015
25 Heath-Brown D R. The size of Selmer groups for the congruent number problem, II. Invent Math, 1994, 118: 331–370. With an appendix by Monsky P
26 Kane D. On the ranks of the 2-Selmer groups of twists of a given elliptic curve. Algebra Number Theory, 2013, 7: 1253–1279
27 de Shalit E. Iwasawa Theory of Elliptic Curves with Complex Multiplication. London: Academic Press, 1987

Congruent number problem and elliptic curves

Ye Tian

Abstract Let n be a positive integer congruent to 5 modulo 8. Assume that all prime factors of n are congruent to 1 modulo 4 and that $\mathbb{Q}(\sqrt{-n})$ has no ideal class of order 4. In this article, we prove that n is a congruent number, i.e., it is the area of a right triangle with rational side-lengths (see Theorem 6.1). Moreover, we also survey results on BSD conjecture and Goldfeld conjecture for congruent elliptic curves $ny^2 = x^3 - x$.

Keywords **congruent numbers, elliptic curves, BSD conjecture, Goldfeld conjecture, Heegner points**

MSC(2010) **11G40, 11G05, 11D25**

doi: 10.1360/N012019-00054