镶嵌数问题及 θ -同余数问题

献给冯克勤教授 80 华诞

何伟^{1,2*}, 胡益榕³, 田野^{3,4,5,6}

1. 清华大学丘成桐数学科学中心, 北京 100084;

2. 北京雁栖湖应用数学研究院, 北京 101408;

3. 中国科学院数学与系统科学研究院, 北京 100190;

4. 中国科学院大学数学科学学院, 北京 100049;

5. 中国科学院晨兴数学中心, 北京 100190;

6. 中国科学院华罗庚数学重点实验室, 北京 100190

E-mail: hewei0714@mail.tsinghua.edu.cn, huyirong20@mails.ucas.ac.cn, ytian@math.ac.cn

收稿日期: 2020-12-31; 接受日期: 2021-03-04; 网络出版日期: 2021-09-29; * 通信作者

国家自然科学基金 (批准号: 11688101) 资助项目

摘要 镶嵌数问题与椭圆曲线的算术紧密相关. 利用 Birch 引理和由本文作者之一田野发展的归纳法来证明 Heegner 点非挠的方法, 本文给出一类多个素因子的镶嵌数的构造, 并且证明相关椭圆曲线的 BSD 猜想 2- 部分. 本文处理的椭圆曲线二次扭族不带复乘, 且其 2-Selmer 群的分布不被已知的猜想和结论所预测.

关键词 镶嵌数 椭圆曲线 BSD 猜想 Waldspurger 公式 Gross-Zagier 公式

MSC (2020) 主题分类 11G40, 11G05, 11D25

1 引言

一个重要的组合问题是, 对一个给定的正整数 n , 判断是否可以将正三角形分割成 n 个全等三角形 (参见文献 [1]). 容易看出, 若正三角形可以被分割成 n 个全等三角形, 那么对任意正整数 k , 正三角形也可以被分割成 nk^2 个全等的三角形. 称一个正整数 n 为镶嵌数, 若存在某个正整数 k 使得正三角形可以被分割成 nk^2 个全等的三角形. 显然一个正整数是否为镶嵌数只依赖其平方自由部分.

镶嵌数问题与 θ -同余数问题相关, 后者是同余数的推广. 一个正整数 n 称为 θ -同余数, 若存在一个有理边长三角形使得有一个角为 θ , 且若记 $\cos \theta = \frac{a}{b}$, $a, b \in \mathbb{Z}$, $(a, b) = 1$, 则其面积为 $n \cdot \sqrt{b^2 - a^2}$. 我们也称 $\frac{\pi}{2}$ -同余数为同余数, 即 n 是同余数当且仅当其是一个有理直角三角形的面积. n 是镶嵌数当且仅当 n 是 $\frac{2\pi}{3}$ -或 $\frac{\pi}{3}$ -同余数 (参见文献 [2]).

英文引用格式: He W, Hu Y R, Tian Y. Tiling number problem and θ -congruent number problem (in Chinese). Sci Sin Math, 2021, 51: 1579–1594, doi: 10.1360/SSM-2020-0354

我们有如下基本问题:

- (1) 判断一个给定的正整数 n 是否为镶嵌数;
- (2) 镶嵌数的分布;
- (3) 构造给定素因子个数的无平方因子的镶嵌数.

对于 θ - 同余数, 也可以提出类似的问题. 这些问题与椭圆曲线的算术直接相关 (参见文献 [2]).

对于一条给定的椭圆曲线 $A/\mathbb{Q}$, 它有如下两个重要的不变量:

- Mordell-Weil 群 $A(\mathbb{Q})$, 这是一个有限生成的交换群, 称其自由部分的秩 $\text{rank}_{\mathbb{Z}}(A(\mathbb{Q}))$ 为 A 的代数秩;
- Hasse-Weil L- 函数 $L(s, A)$, 其有解析延拓且满足函数方程

$$N^{s/2}(2\pi)^{-s}\Gamma(s)L(s, A) = \epsilon \cdot N^{(2-s)/2}(2\pi)^{-(2-s)}\Gamma(2-s)L(2-s, A),$$

其中 N 为 A 的导子, 称 $\epsilon \in \{\pm 1\}$ 为根数, 称 $L(s, A)$ 在 1 处的零点阶数 $\text{ord}_{s=1}L(s, A)$ 为 A 的解析秩.

对一个非零有理数 n , 记 $A^{(n)}$ 为 A 的关于 $\mathbb{Q}(\sqrt{n})$ 的二次扭, 它为 $\mathbb{Q}$ 上的一条椭圆曲线且做基变换到 $\mathbb{Q}(\sqrt{n})$ 上和 A 做相同的基变换后同构. 对一个无平方因子的大于 3 的正整数 n , 其为一个镶嵌数当且仅当 $\mathbb{Q}$ 上椭圆曲线

$$E: y^2 = x(x-1)(x+3)$$

的两个二次扭 $E^{(\pm n)}$ 中至少有一个代数秩为正 (参见文献 [3]).

BSD 猜想秩部分断言一条椭圆曲线 $A/\mathbb{Q}$ 的代数秩 $\text{rank}_{\mathbb{Z}}(A(\mathbb{Q}))$ 和解析秩 $\text{ord}_{s=1}L(s, A)$ 相等. 解析秩的奇偶性可以由根数判断, 当根数为 1 时, 解析秩为偶数; 当根数为 -1 时, 解析秩为奇数. 从而, 猜测当 $E^{(n)}$ 或 $E^{(-n)}$ 的根数为 -1 时, n 为一个镶嵌数. 当根数为 $+1$ 时, 关于镶嵌数对应椭圆曲线二次扭族的 Tunnell 类型的定理 [4,5] 可以用来判断 $E^{(n)}$ ($n \in \mathbb{Z}$) 的解析秩是否大于 0.

一般地, Goldfeld 猜想断言一个椭圆曲线的二次扭族中符号为 $+1$ 的椭圆曲线其秩按照概率 100% 为 0, 符号为 -1 的椭圆曲线其秩按照概率 100% 为 1. 关于镶嵌数对应椭圆曲线二次扭族, 有如下结论: 对一个平方自由的正整数 n ,

- $L(s, E^{(n)})$ 的根数为 -1 当且仅当 $n \equiv 6, 10, 11, 13, 17, 18, 21, 22, 23 \pmod{24}$;
- $L(s, E^{(-n)})$ 的根数为 -1 当且仅当 $n \equiv 5, 9, 10, 15, 17, 19, 21, 22, 23 \pmod{24}$.

关于镶嵌数的具体构造, 已经被许多人研究过, 如 Yoshida [6] 和 Kan [7]. 他们通过 Heegner 点的非平凡性证明了对任意素数 $p \equiv -1 \pmod{24}$, $E^{(\pm p)}$ 的代数秩都为 1. 本文, 我们将文献 [8,9] 中引入的用归纳法来研究多个素因子情形的方法推广应用到镶嵌数情形. 以下是本文的主要结果.

定理 1.1 令 n 为一个无平方因子的正整数, 满足下面条件:

- (1) $n \equiv -1 \pmod{24}$ 且其每个素因子 $\equiv \pm 1 \pmod{24}$;
- (2) 虚二次域 $\mathbb{Q}(\sqrt{-n})$ 的类群没有 4 阶元,

则对 $A = E^{(\pm n)}$, 有

- (1) A 的 BSD 猜想秩部分成立:

$$\text{rank}_{\mathbb{Z}}(A(\mathbb{Q})) = 1 = \text{ord}_{s=1}L(s, A);$$

- (2) A 的 BSD 公式 2- 部分成立且其 Sha 群的阶 $\#\text{III}(A/\mathbb{Q})$ 为奇数.

镶嵌数或更一般的 θ 同余数问题对应于某些椭圆曲线二次扭族的算术性质. 镶嵌数对应的椭圆曲线二次扭族与人们之前研究的二次扭族相比有许多很不一样的性质. 例如, 这个扭族不带有复乘; $\#E(\mathbb{Q})[2] = 4$ 且 E 有一个有理 4- 循环同源. 一般地, 对于椭圆曲线 $A/\mathbb{Q}$, 若 A 没有 2 阶有理挠点, 或 $\#A(\mathbb{Q})[2] = 4$ 且 A 没有有理 4- 循环同源, 则 A 的二次扭族 2-Selmer 群甚至 2^∞ -Selmer 群的分布已经研究得很清楚 (参见文献 [10]), 其满足一般的猜想 (参见文献 [11]). 但是对于镶嵌数对应的二次扭族, 我们甚至还没有一个其 2-Selmer 群分布的猜想.

现在概述通过构造非平凡 Heegner 点来构造镶嵌数的方法. 令 A 为一个导子是 N 的椭圆曲线, K 为一个判别式为 D 的虚二次域且使得 (A, K) 满足经典的 Heegner 假设, 即任意整除 N 的素数都在 K 中分裂. 从而 K 的整数环 $\mathcal{O}_K$ 中存在一个范为 N 的理想 $\mathcal{N}$ 使得 $\mathcal{O}_K/\mathcal{N} \simeq \mathbb{Z}/N\mathbb{Z}$. 通过模参数化 $f: X_0(N) \rightarrow A$ 和复乘理论可构造 Heegner 点

$$y_K = \text{Tr}_{H_K/K} f(P) \in A(K),$$

这里 H_K 为 K 的 Hilbert 类域,

$$P := (\mathbb{C}/\mathcal{O}_K \rightarrow \mathbb{C}/\mathcal{N}^{-1}) \in X_0(N)(H_K).$$

Gross-Zagier (参见文献 [12]) 和 Kolyvagin^[13] 的深刻定理说明, 若 y_K 是非挠的, 则 $A^{(D)}$ 的代数秩和解析秩都为 1. 且也有精确公式将 $L'(1, A^{(D)})$ 和 y_K 的 Néron-Tate 高度联系起来 (参见文献 [14]). 例如, 对 $A = E^{(-1)}$, $K = \mathbb{Q}(\sqrt{-n})$ 使得 $n \equiv -1 \pmod{24}$. 若 y_K 非挠, 则 $E^{(n)}$ 的代数秩与解析秩均为 1, 从而 n 是镶嵌数.

现在问题归结到如何构造 K 使得 y_K 非挠. 当 y_K 不是挠点时, Gross-Zagier 公式和一般的精确 BSD 猜想预言: 当 Sha 群 2- 部分平凡时 (这可以由 2 递降方法检验, 参见命题 4.1), y_K 的 2 可除性本质上等于 Tamagawa 数 $\prod_{\ell} c_{\ell}(A^{(D)})$ 关于 4 的阶. 若 $\#A(\mathbb{Q})[2] = 4$, 则由亏格 (genus) 理论可知 y_K 的 2 不可除性应该与 $\text{ord}_2 \#(\text{Cl}(K)/2\text{Cl}(K)) = \mu(D) - 1$ 很接近, 其中 $\mu(\cdot)$ 代表素因子个数.

我们通过考虑 Heegner 点 y_K 和其扭

$$y_{\chi} = \sum_{\sigma \in \text{Gal}(H_K/K)} \chi(\sigma) f(P)^{\sigma}$$

之间的关系来证明上述猜测, 其中 χ 跑遍所有 $\text{Gal}(H_K/K)$ 的二次特征. 更精确地, 令 $H_0 \subset H_K$ 为由关系 $\text{Gal}(H_K/H_0) \simeq 2\text{Cl}(K)$ 确定的子域, 称为亏格子域, 考虑在文献 [8] 中引入的亏格点 y_0 , 则有如下亏格特征对应的点间的关系:

$$y_K + \sum_{1 \neq \chi \in \widehat{\text{Gal}}(H_0/K)} y_{\chi} = [H_0 : K] \cdot y_0.$$

每个 χ 给出了一个虚二次域 $K_{\chi} = \mathbb{Q}(\sqrt{D_{\chi}})$, 其中 $K(\sqrt{D_{\chi}}) = H_0^{\ker \chi}$ 且 D_{χ} 为一个基本判别式.

在与 Birch 引理类似的假设下, 可以明确地知道上述等式右端的 2 不可除性为 $\mu(D) - 1$. 通常 D_{χ} 的素因子个数严格少于 D . 为了构造非平凡的 y_K , 我们希望通过说明 y_{χ} ($\chi \neq 1$) 为误差项, 从而 y_K 的 2 可除性就和上述 $[H_0 : K] \cdot y_0$ 的 2 可除性相同. 若假设 $L(1, A) \neq 0$ 且当 $L(s, A, \chi)$ 的符号为 -1 时, (A, K_{χ}) 也满足 Heegner 假设, 则 y_{χ} 非挠蕴涵了 $y_{K_{\chi}}$ 非挠且它们落在同一个一维 $\mathbb{Q}$ 线性空间 $A(H_0)_{\mathbb{Q}}^{\chi} = A(K_{\chi})_{\mathbb{Q}}$. 我们希望通过考察 y_{χ} 与 $y_{K_{\chi}}$ 的关系以及对 $y_{K_{\chi}}$ 应用归纳假设来探讨 y_{χ} 的 2 可

除性. 事实上, 我们可以通过考察这两个点的高度关系来考察这两点的比率. 由 Gross-Zagier 公式^[14]可知, $\frac{\hat{h}_Q(y_\chi)}{\hat{h}_Q(y_{K_\chi})}$ 和 $\mathcal{L}(D/D_\chi)^2$ 很接近, 其中

$$\mathcal{L}(D/D_\chi) := \sqrt{\frac{\sqrt{D/D_\chi} L(1, A^{(D/D_\chi)})}{L(1, A)}} \in \mathbb{Q}.$$

为了说明 y_χ 为误差项, 我们需要得到关于 $\mathcal{L}(D/D_\chi)$ 的好的 2- 进赋值下界估计. 一个困难是, 在归纳的过程中, 我们在某些情形需要的 $\mathcal{L}(D/D_\chi)$ 的 2- 进赋值的下界足够大使得有 $L(1, A^{(D/D_\chi)}) = 0$, 或 $L(1, A^{(D/D_\chi)}) \neq 0$ 且此时根据 BSD 猜想所预言, Sha 群 2- 部分必须非平凡. 此时, 我们需要寻找 $m \in \mathbb{Z}_{>0}$ 使得

$$\text{rank}_{\mathbb{F}_2}(\text{Sel}_2((A^{(m)}/\mathbb{Q})) / (A^{(m)}(\mathbb{Q})[2])) > 0.$$

令人意外的是, 我们发现这样的 m 在某个剩余类中概率是 100%, 见命题 4.2.

关于 $\mathcal{L}(D/D_\chi)$ 的 2- 进赋值下界估计通常有几种方式. 然而, 用通常模符号^[15]的方法得到的估计远远不够用. 这里采用与文献 [9] 相同的通过对环面积分做归纳法来估计其 2- 进赋值的方法. 这时就有另外一个困难, $A^{(n)}$ 和 $A^{(-n)}$ 并不同构, 这时需要考察更精确的亏格特征对应的周期之间的关系使得只有一个非误差项出现.

2 环面周期

2.1 Waldspurger 公式

令 A 为一条定义在 $\mathbb{Q}$ 上的椭圆曲线, 其导子为 N . 令 K 为一个虚二次域, 其判别式为 D . 令 χ 为 K 上的一个有限阶非分歧特征.

假设 Rankin-Selberg L- 函数 $L(s, A, \chi)$ 的符号为 $+1$. 由 Tunnell-Saito 条件知, 这决定了一个定义在 $\mathbb{Q}$ 上的正定四元数代数 B 和一个嵌入 $K \rightarrow B$. 由文献 [14] 可知 B 中存在一个判别式为 N 的阶 R 且满足 $R \cap K = \mathcal{O}_K$. 考虑 Π 为 $B_{\mathbb{A}}^\times$ 上的自守表示且满足其在 GL_2 上的 Jacquet-Langlands 对应为 A 对应的自守表示, 则存在唯一的一个一维空间 (参见文献 [14, 命题 3.7]) $\mathbb{C} \cdot f \subset \Pi^{\hat{R}^\times}$ 满足 $\prod_{p|(N,D)} K_p^\times$ 通过 χ^{-1} 作用. f 可看作 Shimura 集 $X = B^\times \backslash \hat{B}^\times / \hat{R}^\times$ 上的函数.

固定上述 Shimura 集的代表元 $X = \{[g_i]\}$, $g_i \in \hat{B}^\times$. Shimura 集 X 的复值函数空间上有一个 Hermite 内积结构

$$\left\langle \sum_i a_i [g_i], \sum_i b_i [g_i] \right\rangle = \sum_i \frac{1}{w_i} a_i \bar{b}_i,$$

其中 $w_i = [g_i \hat{R}^\times g_i^{-1} \cap B^\times : \pm 1]$. 定义 f 和 χ 对应的环面周期为

$$P_\chi(f) := \sum_{t \in \text{Cl}(K)} \chi(t) f(t).$$

Waldspurger 公式叙述如下:

定理 2.1 (参见文献 [14, 定理 1.8]) 记号如上, 有

$$L(1, A, \chi) = 2^{-\mu(N,D)} \frac{8\pi^2(\phi, \phi)_{\Gamma_0(N)}}{[\mathcal{O}_K^\times : \mathbb{Z}^\times]^2 \sqrt{|D|}} \frac{|P_\chi(f)|^2}{\langle f, f \rangle},$$

其中 ϕ 为对应于 A 的新形式, $(\cdot, \cdot)_{\Gamma_0(N)}$ 为 $X_0(N)$ 上的 Petersson 内积, $\mu(N, D)$ 为 (N, D) 的素因子个数.

2.2 归纳结构

令 H_0 为 H_K 的亏格子域.

命题 2.1 (亏格理论) • $[H_0 : K] = 2^{\mu(D)-1}$;

- $H_0 = K(\sqrt{p_i^*})$, 其中 p_i 跑遍所有 D 的奇素因子且 $p_i^* = (-1)^{\frac{p_i-1}{2}} p_i$;
- 有如下两个集合间的一一对应:
- $\text{Gal}(H_0/K)$ 的特征 χ_d

和

- D 的因子 d (满足 $d < 0$ 且 d 为基本判别式)

对应关系为

$$K(\sqrt{d}) = H_0^{\ker \chi_d}.$$

假设 $L(s, A, \mathbf{1}_K)$ 符号为 1, 令 f 为上一小节对应于 $(A, \chi = \mathbf{1}_K)$ 的测试向量. 通过类域论可以将 $\text{Cl}(K)$ 和 $\text{Gal}(H_K/K)$ 等同. 令

$$y_{\chi_d} = \sum_{t \in \text{Cl}(K)} \chi_d(t) f(t), \quad K_d = \mathbb{Q}(\sqrt{d}), \quad y_d = \sum_{t \in \text{Cl}(K_d)} f(t).$$

令 H'_0 为 H_0 的一个满足

$$\begin{cases} [H_0 : H'_0] = 2, & H_0 = H'_0(i), \text{ 若 } 4 \parallel D, \\ H_0, & \text{其他情形} \end{cases}$$

的子域.

令 $y_0 = \sum_{\sigma \in \text{Gal}(H_K/H'_0)} f(\sigma)$, 称其为亏格周期. 我们有如下的亏格特征对应的周期间的关系:

$$y_D + \sum_{\mathbf{1} \neq \chi_d \in \widehat{\text{Gal}}(H'_0/K)} y_{\chi_d} = [H'_0 : K] y_0.$$

假设 $L(1, A) \neq 0$, 且对每个上述求和中的 y_{χ_d} , 当 $y_{\chi_d} \neq 0$ 时, $(A, \mathbf{1}_{K_d})$ 和 $(A, \mathbf{1}_K)$ 对应相同的测试向量. 注意到当 $y_{\chi_d} \neq 0$ 时, f 也是上一小节中 (A, χ_d) 对应的测试向量, 则由精确 Waldspurger 公式得

$$y_{\chi_d} = \mathcal{L}\left(\frac{D}{d}\right) \frac{\epsilon_d[\mathcal{O}_K^\times : \mathbb{Z}^\times]}{[\mathcal{O}_{K_d}^\times : \mathbb{Z}^\times]} y_d,$$

其中

$$\mathcal{L}\left(\frac{D}{d}\right) := \sqrt{\frac{2^{\mu(N, D/d)} \sqrt{D/d} L(1, A^{(D/d)})}{L(1, A)}} \in \mathbb{Q},$$

$\epsilon_d \in \{\pm 1\}$. 我们有如下更精确的不同虚二次域对应的周期间的关系.

命题 2.2 假设

- $L(1, A) \neq 0$, $L(s, A, \mathbf{1}_K)$ 的符号为 1;
 - 对任意 $d \mid D$, $d < 0$ 为一个基本判别式, 当 $y_{\chi_d} \neq 0$ 时, $(A, \mathbf{1}_{K_d})$ 和 $(A, \mathbf{1}_K)$ 共享相同的测试向量,
- 则有

$$y_D + \sum_d y_d \cdot \mathcal{L}\left(\frac{D}{d}\right) \frac{\epsilon_d[\mathcal{O}_K^\times : \mathbb{Z}^\times]}{[\mathcal{O}_{K_d}^\times : \mathbb{Z}^\times]} = [H'_0 : K] y_0,$$

其中 d 满足 $1 \neq \chi_d \in \widehat{\text{Gal}}(H'_0/K)$,

$$\epsilon_d = \begin{cases} 0, & \text{若 } y_{\chi_d} = 0, \\ \pm 1, & \text{其余情形.} \end{cases}$$

证明 我们有如下亏格特征对应的周期间的关系:

$$y_D + \sum_d y_{\chi_d} = [H'_0 : K] y_0,$$

其中 d 满足 $1 \neq \chi_d \in \widehat{\text{Gal}}(H'_0/K)$. 通过应用 Waldspurger 公式, 可得

$$y_D + \sum_d y_d \cdot \mathcal{L}\left(\frac{D}{d}\right) \cdot \frac{\epsilon_d [\mathcal{O}_K^\times : \mathbb{Z}^\times]}{[\mathcal{O}_{K_d}^\times : \mathbb{Z}^\times]} = [H'_0 : K] y_0.$$

证毕. □

注 2.1 若 f 取值为奇数, 则由亏格理论知 $2^{\mu(D)-1}$ 整除等式右端. 这里介绍 H'_0 的目的是使得只有一个非误差项出现在左端等式中, 从而可以应用归纳法.

假设 n 为一个使得 $A^{(n)}$ 的符号为 $+1$ 的整数, 定义解析 Sha 为

$$\mathcal{L}(A^{(n)}) := \frac{L(1, A^{(n)})}{\Omega(A^{(n)})} \cdot \frac{\#(A^{(n)}(\mathbb{Q})_{\text{tor}})^2}{\prod_{\ell} c_{\ell}(A^{(n)})}.$$

假设 m 为 r 个不同素数乘积, $m \equiv 1 \pmod{24}$ 且每个素因子 $\ell_i \equiv \pm 1 \pmod{24}$. 令 $E/\mathbb{Q}$ 为椭圆曲线 $y^2 = x(x-1)(x+3)$.

命题 2.3 对 $r \geq 1$ 和 $\epsilon = \pm 1$, 有

$$\mathcal{L}(E^{(\epsilon m)}) \in 2^{1-\epsilon} \mathbb{Z}.$$

注 2.2 上述命题有如下等价形式: 对于 $A = E^{(\epsilon)}$, $\epsilon \in \{\pm 1\}$, 有

$$\mathcal{L}(m) \in 2^{r+1} \mathbb{Z}.$$

我们通过考察不同虚二次域对应的周期间的关系, 应用 Waldspurger 公式和归纳法对上述命题给出证明.

事实 2.1 (Eichler-Siegel 权重公式 [16]) 令 B 为 $\mathbb{Q}$ 上一个正定四元数代数, $\mathcal{O}_B$ 为一个极大阶, 则对任意阶 $R \subset \mathcal{O}_B$, 有

$$\sum \frac{1}{w_i} = |\zeta(-1)| \prod_{p: B_p \text{ 分歧}} (p-1) \cdot [\widehat{\mathcal{O}}_B^\times : \widehat{R}^\times].$$

考虑定义在 $\mathbb{Q}$ 上只在 3 和 ∞ 分歧的四元数代数 $B = \mathbb{Q} \oplus \mathbb{Q}i \oplus \mathbb{Q}j \oplus \mathbb{Q}k$, 其中 $i^2 = -1$, $j^2 = -3$, $k = ij = -ji$. 一个极大阶 $\mathcal{O}_B$ 为 $\mathbb{Z}[i, \frac{1+i}{2}, i\frac{1+i}{2}]$. 令 $R^- = \mathbb{Z}[i] + 2(1+i)\mathcal{O}_B$ 是判别式为 24 的阶, $R^+ = \mathbb{Z}[i] + 4\mathcal{O}_B$ 是判别式为 48 的阶. 记 X^ϵ 为 Shimura 集 $B^\times \backslash \widehat{B}^\times / \widehat{R}^{\epsilon, \times}$. 固定一组 X^ϵ 的代表元 $X^\epsilon = \{[g_i^\epsilon]\}$, 令 $w_i^\epsilon = [g_i^\epsilon \widehat{R}^{\epsilon, \times} g_i^{\epsilon, -1} \cap B^\times : \pm 1]$.

引理 2.1 (1) $\#X^+ = 4$, $\#X^- = 2$;

(2) 对 $\epsilon = \pm 1$, $w_i^\epsilon = 2$;

(3) 文献 [14] 中对应于 $(E^{(-\epsilon)}, \mathbf{1}_{\mathbb{Q}(i)})$ 的测试向量空间由如下 ($\mathbb{Z}$ 本原的) 测试向量 f^ϵ 生成, 其中 $f^- = (1, -1)$ 且 $f^+ = (1, 1, -1, -1)$.

证明 直接计算可得

$$\begin{aligned} [\mathrm{GL}_2(\mathbb{Z}_2) : 1 + 4M_2(\mathbb{Z}_2)] &= 16 \times 6, \quad [(\mathbb{Z}[\mathrm{i}] + 4\mathcal{O}_{B_2})^\times : 1 + 4\mathcal{O}_{B_2}] = 8, \\ \mathcal{O}_B^\times &= \left\{ \pm 1, \pm \mathrm{i}, \pm \frac{1 \pm \mathrm{j}}{2}, \pm \frac{\mathrm{i}(1 \pm \mathrm{j})}{2} \right\}, \\ ((\mathbb{Z}[\mathrm{i}] + 4\mathcal{O}_{B_2})^\times \cap \mathcal{O}_B^\times) &= \{\pm 1, \pm \mathrm{i}\}. \end{aligned}$$

故由 B 的类数为 1 可知 $\#X^+ = 4$. 注意到 $(1 + 2(1 + \mathrm{i})\frac{1+\mathrm{j}}{2})_2$ 在 X^+ 中非平凡但是在 X^- 中平凡, 故 $\#X^- = 2$. 由上述 Eichler-Siegel 权重公式可得

$$\sum \frac{1}{w_i^\epsilon} = |\zeta(-1)| \prod_{p: B_p \text{ 分歧}} (p-1) [\widehat{\mathcal{O}}_B^\times : \widehat{R}^{\epsilon, \times}],$$

从而可知 $w_i^\epsilon = 2$, $\epsilon = \pm 1$.

故可以选取 $f^- = (1, -1)$.

不妨设 $f^+ = (a, -a, b, -b)$, 其中 $(a, b) = 1$, $a, b \in \mathbb{Z}$ 且 $f^+(1) = a$. 对 $(E^{(-1)}, \mathbb{Q}(\mathrm{i}))$ 应用 Waldspurger 公式, 结合事实 $L^{\mathrm{alg}}(1, E) = \frac{1}{8}$ 和 $L^{\mathrm{alg}}(1, E^{(-1)}) = \frac{1}{4}$ 可知,

$$\frac{|P_{\mathbf{1}_{\mathbb{Q}(\mathrm{i})}}(f^+)|^2}{\langle f^+, f^+ \rangle} = \frac{1}{2},$$

即 $a^2 + b^2 = 2a^2$. 故必须有 $|a| = |b| = 1$. □

命题 2.3 的证明 固定 ϵ , 考虑

$$(A = E^{(-\epsilon)}, \chi = \mathbf{1}_{\mathbb{Q}(\sqrt{-m})}),$$

其对应的测试向量为 f^ϵ . 由 Waldspurger 公式知, 当 $r \geq 1$ 时, 有

$$\frac{L(1, E^{(\epsilon m)})}{\Omega(E^{(\epsilon m)})} = \frac{P_{\mathbf{1}_K}(f^\epsilon)^2}{\langle f^\epsilon, f^\epsilon \rangle}.$$

我们有

$$P_{\mathbf{1}_K}(f^\epsilon)^2 = 4^{r-1} \cdot 2^{1+\epsilon} \mathcal{L}(E^{(\epsilon m)}).$$

故需要证明

$$P_{\mathbf{1}_K}(f^\epsilon) \in 2^r \mathbb{Z}.$$

当 $r = 1$ 时, 这可由 $2 \mid \#\mathrm{Cl}(K)$ 得到.

我们将会对 y_{χ_d} 、 y_d 和 y_0 中添加上标 ϵ 用来区分它们是由测试向量 f^ϵ 所定义出来的. 由不同虚二次域对应的点间的关系知,

$$y_{-4m}^\epsilon + \sum_d y_d^\epsilon \cdot \epsilon_d \mathcal{L}\left(\frac{D}{d}\right) = [H'_0 : K] y_0^\epsilon,$$

这里 $d < 0$ 跑遍所有 D 的真因子且满足

- d 为一个基本判别式;
- $\chi_d \in \widehat{\mathrm{Gal}}(H'_0/K)$.

注意到当 $|d| \equiv 3 \pmod{4}$ 时, 由于 $E^{(-\epsilon D/d)}$ 根数为 -1 , 故 $L(1, E^{(-\epsilon D/d)}) = 0$. 从而

$$y_{-4m}^\epsilon + \sum_{\substack{4|d|D, d<0 \\ d \text{ 为基本判别式,} \\ 1 \neq \chi_d \in \widehat{\text{Gal}}(H'_0/K)}} y_d^\epsilon \cdot \epsilon_d \mathcal{L}\left(\frac{D}{d}\right) = [H'_0 : K] y_0^\epsilon.$$

由于 $f^\epsilon \equiv 1 \pmod{2}$ 且 $2 \mid \#\text{Gal}(H_K/H'_0)$, 因此有 $2 \mid y_0^\epsilon$. 故由亏格理论有 $2^r \mid [H'_0 : K] y_0^\epsilon$.

注意到由 $\chi_d \in \widehat{\text{Gal}}(H'_0/K)$ 可得 $d \neq -4$. 由于 $2 \mid y_0^\epsilon$, 因此命题可由注 2.2 和归纳法得到. $\square$

3 Heegner 点

3.1 Gross-Zagier 公式

令 $N \geq 1$ 为一个整数. 模曲线 $X_0(N)$ 为定义在 $\mathbb{Q}$ 上的一条射影代数曲线且

$$X_0(N)(\mathbb{C}) = \Gamma_0(N) \backslash \mathcal{H} \sqcup \mathbb{P}^1(\mathbb{Q}),$$

其中 $\mathcal{H}$ 为上半平面. 它的仿射部分 $Y_0(N)$ 有如下的模解释: 对 $\mathbb{C}$ 的任意一个子域 F , $Y_0(N)(F)$ 参数化了定义在 F 上的带有一个 N -同源的椭圆曲线同构类.

令 A 为一条导子是 N 的椭圆曲线, K 为一个虚二次域且满足经典的 Heegner 假设, 即任意 N 的素因子都在 K 中分裂. 令 χ 为 K 上的一个有限阶非分歧 Hecke 特征, 则 Rankin-Selberg L -函数 $L(s, A, \chi)$ 的符号为 -1 且我们有一个模参数化

$$f : X_0(N) \rightarrow A, \quad [\infty] \mapsto O.$$

令 $\mathcal{N} \subset \mathcal{O}_K$ 为满足 $\mathcal{O}_K/\mathcal{N} \cong \mathbb{Z}/N\mathbb{Z}$ 的一个整理想. 由复乘理论知, 同源

$$P : \mathbb{C}/\mathcal{O}_K \longrightarrow \mathbb{C}/\mathcal{N}^{-1}$$

实际上定义了 $X_0(N)$ 的一个 H_K 点. 定义对应于 (A, χ) 的 Heegner 点为

$$y_\chi := \sum_{t \in \text{Cl}(K)} \chi(t) f(P)^{\sigma_t},$$

这里 σ_t 为 t 的通过类域论给出的在 K 的 Hilbert 类域对 K 的 Galois 群中的像.

记 D 为 K 的判别式. 令 ϕ 为 A 对应的权为 2、水平为 N 的新形式.

精确 Gross-Zagier 公式叙述如下:

命题 3.1 (参见文献 [14, 定理 1.5]) Gross-Zagier 公式叙述如下:

$$L'(1, A, \chi) = \frac{8\pi^2(\phi, \phi)_{\Gamma_0(N)}}{[\mathcal{O}_K^\times : \mathbb{Z}^\times]^2 \sqrt{|D|}} \cdot \frac{\widehat{h}_K(y_\chi)}{\deg f},$$

其中 $\widehat{h}_K$ 为 E/K 上的 Néron-Tate 高度配对.

3.2 Birch 引理

令 (A, K, χ) 如上小节. 当 χ 平凡时, 将 y_χ 记为 y_K .

如下的 Birch 引理说明了当 $\text{Cl}(K)$ 没有 4 阶元且 $T := f([0])$ 在 $A(\mathbb{Q})_{\text{tor}}$ 中 2 不可除时, 对应的 Heegner 点是非挠的 (参见文献 [17]).

引理 3.1 (Birch 引理) 假设 $D = -p$, 其中 $p \equiv 3 \pmod{4}$ 为一个素数; $T \notin 2A(\mathbb{Q})$, 则 $y_K \in A(K)$ 为无穷阶元素.

更进一步地, 令 a 为一个奇数且使得 $aA(K)_{\text{tor}} \subset A(K)[2^\infty] = A(\mathbb{Q})[2^\infty]$, 则

$$z := a(2y_K - \#\text{Cl}(K)T) \in A(K)^- \setminus (2A(K)^- + A(K)_{\text{tor}}^-).$$

特别地, $A^{(-p)}$ 的解析秩为 1.

证明 注意到 $f(P^w) - \epsilon f(P) = T$ 为一个常值映射, 其中 w 为 Fricke 对合变换且 $-\epsilon$ 为 $L(s, A)$ 的函数方程的符号. 由于 $T \neq O$, 通过取 P 为 w 的固定点可知 $\epsilon = -1$. 由 w 在复乘点上的作用 (参见文献 [18]) 可知,

$$y_K + \bar{y}_K = h_K T,$$

这里 h_K 为 K 的类数. 令 a 为满足 $aA(K)_{\text{tor}} = A(\mathbb{Q})_{\text{tor}}[2^\infty]$ 的一个奇数, 则 $a(y_K + \bar{y}_K) = ah_K T \in A(\mathbb{Q})[2^\infty]$. 故

$$z := a(2y_K - h_K T) \in A(K)^-.$$

假设 $z = 2z_1 + S \in 2A(K)^- + A(K)_{\text{tor}}^-$, 其中 $z_1 \in A(K)^-$ 且 $S \in A(K)_{\text{tor}}^-$, 则 $2z_1 + S = z = a(2y_K - h_K T)$ 推出 $2a(ay_K - z_1) = a(S + ah_K T) \in A(K)[2^\infty]$, 故有

$$S_1 := a(ay_K - z_1) \in A(\mathbb{Q})[2^\infty].$$

现在有

$$a^2 h_K T = a^2 (y_K + \bar{y}_K) = 2S_1 \in 2A(\mathbb{Q})_{\text{tor}},$$

这与 $T \notin 2A(\mathbb{Q})$ 矛盾. □

命题 3.2 (参见文献 [19, 定理 3.2.16]) 令 $N > 1$ 为一个整数, 则 $X_0(N)$ 的 Jacobi 簇 $J_0(N)$ 上由度数 0 除子 $[0] - [\infty]$ 定义的挠点定义在 $\mathbb{Q}$ 上且其阶为 $k(N)/m(N)$. 这里, 若 $N = \prod_{p|N} p^{n_p}$ 为 N 的因子分解, $N_0 := \prod_{p|N} p$, 则 $k(N) = N \prod_{p|N} (p - p^{-1})$ 且 m 为 $k(N)$ 、 $12w_p$ ($p|N$) 和 $24r_d$ ($d|N$) 的最大公因子, 其中

- 对每个 $p|N$, $w_p = (n_p p - n_p + 2) \prod_{p' \neq p, p'|N} (p' - 1)$;
- 对每个 $d|N$, $d > 0$, 令 μ 为 Mobius 函数, $r_d = s_d - s_{N/d}$, $s_d = N_0 \mu(d)/d$.

椭圆曲线 $E: y^2 = x(x-1)(x+3)$ 的导子为 24 且模曲线 $X_0(24)$ 的亏格为 1, 故 $E = (X_0(24), [\infty])$. 由命题 3.2, 有以下推论:

推论 3.1 我们有 $f: (X_0(24), [\infty]) \simeq (E, O)$, 且点 $f([0])$ 的阶为 4 且满足 Birch 引理的假设, 即 $f([0]) \notin 2E(\mathbb{Q})$.

回顾关于 L-函数特殊值的一个经典结果.

命题 3.3 (参见文献 [20, 命题 4.8] 和 [21, 注记 2.9]) 令 $\phi \in S_2(\Gamma_0(N))$ 为一个新形式, A 为其对应的 $J_0(N)$ 的最优商. 令 c_A 为 A 对应的 Manin 常数, c_∞ 为 $A(\mathbb{R})$ 的连通分支数, 则

$$c_\infty c_A L(1, A) / \Omega(A)$$

的分母整除 $J_0(N)$ 上挠点 $[0] - [\infty]$ 在 A 中像的阶数, 且当 $L(1, A) \neq 0$ 、 A 为椭圆曲线时, 两者相等.

注意到 $E^{(-1)}$ 的导子为 48, 且为 $J_0(48)$ 的最优商. 对应的模参数化 $f: X_0(48) \rightarrow E^{(-1)}$ 的度数为 2 且 Manin 常数为 1. 由命题 3.3 和事实 $\frac{L(1, E^{(-1)})}{\Omega(E^{(-1)})} = \frac{1}{4}$ 有下面的推论:

推论 3.2 令 $f: X_0(48) \rightarrow E^{(-1)}$ 为最优参数化, 则 $f([0])$ 的阶为 2, 故 $f([0]) \notin 2E^{(-1)}(\mathbb{Q})$.

注 3.1 可以通过 $E^{(-6)}$ 对应的模参数化证明对任意一个素数满足 $\ell \equiv -1 \pmod{24}$, 6ℓ 为一个镶嵌数.

3.3 归纳结构

令 $y_0 = \text{Tr}_{H_K/H_0} f(P)$, 称其为亏格点. 对于满足 Heegner 假设的基本判别式 $d < 0$, 记

$$y_d = \sum_{t \in \text{Cl}(K_d)} f(P)^{\sigma_t}.$$

有如下的亏格特征对应的点间的关系:

$$y_D + \sum_d y_{\chi_d} = [H_0 : K] y_0,$$

其中 χ_d 跑遍所有 $\text{Gal}(H_0/K)$ 的非平凡特征. 若对任意满足 y_{χ_d} 非挠的 χ_d , 都有 $(E, \mathbf{1}_{K_d})$ 满足经典的 Heegner 假设, 则由 Gross-Zagier 公式有如下观察:

若 y_{χ_d} 非挠, 则

- y_{K_d} 也非挠且两个点落在同一个一维 $\mathbb{Q}$ 线性空间 $(A(H_0) \otimes \mathbb{Q})^{\chi_d} = A(K_d) \otimes \mathbb{Q}$;
- y_{χ_d} 本质上等于 $\pm \mathcal{L}(D/d) \frac{[\mathcal{O}_K^\times : \mathbb{Z}^\times]}{[\mathcal{O}_{K_d}^\times : \mathbb{Z}^\times]} y_d$, 这里

$$\mathcal{L}\left(\frac{D}{d}\right) := \sqrt{\frac{\sqrt{D/d} L(1, A^{(D/d)})}{L(1, A)}} \in \mathbb{Q}.$$

更精确地, 有如下的不同虚二次域对应的点间的关系:

命题 3.4 假设

- $L(1, A) \neq 0$, $L(s, A, \mathbf{1}_K)$ 的符号为 -1 ;
 - 任意满足 $d \mid D$ 且 $d < 0$ 为基本判别式的整数 d , 当 $L(s, A, \mathbf{1}_{K_d})$ 的符号为 -1 时, (A, K_d) 都满足经典的 Heegner 假设,
- 则等式

$$y_D + \sum_d y_d \cdot \mathcal{L}\left(\frac{D}{d}\right) \cdot \frac{\epsilon_d [\mathcal{O}_K^\times : \mathbb{Z}^\times]}{[\mathcal{O}_{K_d}^\times : \mathbb{Z}^\times]} = [H_0 : K] y_0$$

在相差一个 $E(H_0)$ 中挠点的意义下成立, 这里 $d < 0$, $d \mid D$ 且 $d \neq D$ 跑遍所有基本判别式,

$$\epsilon_d = \begin{cases} 0, & \text{若 } y_{\chi_d} \text{ 为挠点,} \\ \pm 1, & \text{其余情形.} \end{cases}$$

证明 我们有如下亏格特征对应的点间的关系:

$$y_D + \sum_d y_{\chi_d} = [H_0 : K] y_0,$$

其中 $d < 0$ 且 $d \neq D$ 跑遍所有 D 的因子且满足 d 为一个基本判别式. $\chi_d \in \widehat{\text{Gal}}(H_0/K)$ 为 d 对应的特征 (参见 2.1). 由假设, 若 y_{χ_d} 非挠, 则 y_d 非挠且它们落在一维 $\mathbb{Q}$ 线性空间

$$(A(H_K) \otimes \mathbb{Q})^{\chi_d} = A(K_d) \otimes \mathbb{Q}.$$

由 Gross-Zagier 公式, 可得

$$\frac{\widehat{h}_{\mathbb{Q}}(y_{\chi_d})}{\widehat{h}_{\mathbb{Q}}(y_d)} = \frac{\widehat{h}_K(y_{\chi_d})}{\widehat{h}_{K_d}(y_d)} = \mathcal{L}\left(\frac{D}{d}\right)^2 \cdot \frac{[\mathcal{O}_K^{\times} : \mathbb{Z}^{\times}]^2}{[\mathcal{O}_{K_d}^{\times} : \mathbb{Z}^{\times}]^2}.$$

故等式

$$y_D + \sum_d y_d \cdot \mathcal{L}\left(\frac{D}{d}\right) \cdot \frac{\epsilon_d[\mathcal{O}_K^{\times} : \mathbb{Z}^{\times}]}{[\mathcal{O}_{K_d}^{\times} : \mathbb{Z}^{\times}]} = [H_0 : K]y_0$$

在相差 $E(H_0)$ 中挠点意义下成立. $\square$

考虑 $A : y^2 = x(x-1)(x+3)$ 或 $y^2 = x(x+1)(x-3)$. 令 $n = \prod_{i=1}^k \ell_i$ 且满足 $n \equiv -1 \pmod{24}$, $\ell_i \equiv \pm 1 \pmod{24}$, $1 \leq i \leq k$.

我们将会利用 Gross-Zagier 公式、归纳法和上节证明的 L-函数特殊值的估计来证明如下的定理. 注意到该定理被 BSD 猜想所预测.

令 $K = \mathbb{Q}(\sqrt{-n})$, H_0 为其亏格域. 令 $y_{-n} \in A(K)$ 为 $(A, K = \mathbb{Q}(\sqrt{-n}), \mathbf{1}_K)$ 对应的 Heegner 点.

定理 3.1 我们有 $z := (2y_{-n} - \#\text{Cl}(K)f(0)) \in 2^{k-1}A(K)^- + A(K)_{\text{tor}}^-$. 更进一步地, 当 $\text{Cl}(K)$ 没有 4 阶元时, $z \notin 2^k A(K)^- + (A(K)^-)_{\text{tor}}$.

注 3.2 由 Gross-Zagier 公式, 有如下关系:

$$[A^{(-n)}(\mathbb{Q})/A^{(-n)}(\mathbb{Q})_{\text{tor}} : \mathbb{Z}z]^2 = 4^{k-1} \cdot \mathcal{L}'(A^{(-n)}),$$

其中 $\mathcal{L}'(A^{(-n)})$ 为解析 Sha.

证明 注意到如下事实: 当 $p \geq 3$ 时, 模 p 的 Galois 表示 $G_{\mathbb{Q}} \rightarrow \text{Aut}_{\mathbb{F}_p}(A[p])$ 为满射, 则可证明 $A(H_0)_{\text{tor}} = A(\mathbb{Q})[2^{\infty}]$. 现在通过归纳法证明定理.

$k=1$ 时的结论可以直接由 Birch 引理得到. 现在假设 $k > 1$ 且定理对 $r < k$ 都成立.

由不同虚二次域对应的点间的关系, 有

$$y_{-n} + \sum_d y_d \cdot \epsilon_d \mathcal{L}(-n/d) = 2^{k-1}y_0 + \text{tor},$$

其中 $d < 0$, $d \mid -n$ 且满足 $d \neq -n$, d 为一个基本判别式. 故 $|d| \equiv -1 \pmod{24}$ 且 $\mu(d) < \mu(n)$. 由归纳法和环面积分得到 L-函数特殊值的估计, 有

$$2y_d \in 2^{\mu(d)-1}A(H_0) + A(H_0)_{\text{tor}},$$

$$2^{\mu(-n/d)+1} \left| \mathcal{L}\left(-\frac{n}{d}\right) \right|.$$

故由归纳可知, $y_{-n} \in 2^{k-1}A(H_0) + A(H_0)_{\text{tor}}$.

现在令 $z := 2y_{-n} - \#\text{Cl}(K)f(0)$, 则 $z \in A(K)^-$. 故有 $z = 2^{k-1}(2y_0 - [H_K : H_0]f([0]) + 2z') + \text{tor}$, 其中 $z' \in A(H_0)^-$.

断言 $z'' := 2y_0 - [H_K : H_0]f([0]) + 2z' \in A(K)^-$. 事实上, 对任意 $\sigma \in \text{Gal}(H_0/K)$, 都有

$$(\sigma - 1)(y_0 + z') \in A(H_0)_{\text{tor}}.$$

由于 σ 是二阶元, 因此 $(\sigma - 1)(y_0 + z')$ 是一个二阶元. 从而 $z'' \in A(K)^-$, 故 $z \in 2^{k-1}A(K)^- + A(K)_{\text{tor}}^-$.

现在考虑 Heegner 点的精确的 2 可除性. 我们有

$$y_0 + \bar{y}_0 = [H_K : H_0]f([0]) \in A(H_0)_{\text{tor}}.$$

由于 $2 \nmid f(0)$ 且 $A(H_0)_{\text{tor}} = A(\mathbb{Q})[2^\infty]$, 故 $2 \nmid [H_K : H_0]$ 推出 $y_0 \notin 2A(H_0) + A(H_0)_{\text{tor}}$. 假设 $2 \nmid [H_K : H_0]$. 若 $z = 2^k z'' + u$, 其中 $z'' \in A(K)^-$ 且 $u \in A(K)_{\text{tor}}^-$, 则 $z'' - (y_0 + z') \in A(H_0)_{\text{tor}} = A(\mathbb{Q})[2^\infty]$. 所以

$$z'' - y_0 - z' = -z'' - \bar{y}_0 + z',$$

从而 $2(z'' - y_0 - z') = -(y_0 + \bar{y}_0) = -[H_K : H_0]f([0])$, 矛盾. $\square$

4 2- 递降和 2- 部分 BSD 公式

4.1 2- 递降

令 m 为一个平方自由的整数, $E^{(m)}/\mathbb{Q}$ 为椭圆曲线 $y^2 = x(x-m)(x+3m)$. 其 2-Selmer 群定义为

$$\text{Sel}_2(E^{(m)}/\mathbb{Q}) := \text{Ker} \left(H^1(\mathbb{Q}, E^{(m)}[2]) \longrightarrow \prod_v H^1(\mathbb{Q}_v, E^{(m)})[2] \right).$$

令 S 为所有整除 $6m\infty$ 的素数的集合, $\mathbb{Q}(S, 2) \subset \mathbb{Q}^\times/\mathbb{Q}^{\times 2}$ 为支撑在 S 上的子群, 等价地可描述为平方自由的素因子都在 S 中的整数, 则 $\text{Sel}_2(E^{(m)}/\mathbb{Q})$ 中元素可以看作满足 $C_\Lambda(\mathbb{A}_\mathbb{Q}) \neq \emptyset$ 的曲线 $C_\Lambda/\mathbb{Q}$, 这里 $\Lambda = (b_1, b_2) \in \mathbb{Q}(S, 2) \times \mathbb{Q}(S, 2)$,

$$C_\Lambda : \begin{cases} b_1 z_1^2 - b_2 z_2^2 = m t^2, \\ b_1 z_1^2 - b_1 b_2 z_3^2 = -3m t^2. \end{cases}$$

注意到 $C_\Lambda(\mathbb{A}_\mathbb{Q}) \neq \emptyset$ 当且仅当 $C_\Lambda(\mathbb{Q}_S) \neq \emptyset$. 4 个 2- 挠点 $O, (0, 0), (m, 0), (-3m, 0)$ 对应到 $(b_1, b_2) = (1, 1), (-3, -m), (m, 1), (-3m, -m)$.

假设 m 为一个平方自由且和 6 互素的整数. 若 $\Lambda = (b_1, b_2) \in \mathbb{Q}(S, 2) \times \mathbb{Q}(S, 2)$, 则对任意 $p \mid m$, 有 $C_\Lambda(\mathbb{Q}_p) \neq \emptyset$ 当且仅当

$$\begin{cases} \left(\frac{b_1}{p}\right) = \left(\frac{b_2}{p}\right) = 1, & \text{若 } p \nmid b_1 b_2, \\ \left(\frac{m/b_1}{p}\right) = \left(\frac{b_2}{p}\right) = 1, & \text{若 } p \mid b_1, \quad p \nmid b_2, \\ \left(\frac{-3b_1}{p}\right) = \left(\frac{-m/b_2}{p}\right) = 1, & \text{若 } p \nmid b_1, \quad p \mid b_2, \\ \left(\frac{-3m/b_1}{p}\right) = \left(\frac{-m/b_2}{p}\right) = 1, & \text{若 } p \mid b_1, \quad p \mid b_2; \end{cases}$$

$C_\Lambda(\mathbb{Q}_3) \neq \emptyset$ 当且仅当 $3 \nmid b_2$ 且

$$\begin{cases} \left(\frac{b_2}{3}\right) = 1, & \text{若 } 3 \nmid b_1, \\ \left(\frac{-b_2 m}{3}\right) = 1, & \text{若 } 3 \mid b_1. \end{cases} \quad (4.1)$$

从而可知 (i) $C_\Lambda(\mathbb{R}) \neq \emptyset$ 当且仅当

$$\begin{cases} b_1 b_2 > 0, & \text{若 } m > 0, \\ b_2 > 0, & \text{若 } m < 0; \end{cases}$$

(ii) 若 $C_\Lambda(\mathbb{Q}_2) \neq \emptyset$, 则 b_1 必为奇数.

假设 $m = \ell_1 \cdots \ell_k$, 令 $A = (a_{ij}) \in M_{k \times k}(\mathbb{F}_2)$ 为如下方式定义的矩阵: 对任意 $i \neq j$, $a_{ij} := [\frac{\ell_j}{\ell_i}]$ (加法 Legendre 符号) 且对任意 i 有 $\sum_j a_{ij} = 0$. 记 $b_1 = c_1 \prod_i \ell_i^{x_{1,i}}$, $b_2 = c_2 \prod_i \ell_i^{x_{2,i}}$, 其中 $x_{1,i}, x_{2,i} \in \mathbb{F}_2$ 且 $c_i \mid 6$. 记 α_t ($t = 1, 2$) 为由元素 $[\frac{c_t}{\ell_i}]$ 构成的列向量. 对任意整数 d , 令 D_d 为对角矩阵, 其元素为 $[\frac{d}{\ell_i}]$, 则当 $m > 0$ 时, 有等式

$$\begin{pmatrix} A & D_{-3} \\ & A + D_{-1} \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} \alpha_1 \\ \alpha_2 \end{pmatrix},$$

当 $m < 0$ 时,

$$\begin{pmatrix} A + D_{-1} & D_{-3} \\ & A \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} \alpha_1 \\ \alpha_2 \end{pmatrix}.$$

引理 4.1 令 $A = (a_{ij}) \in M_{k \times k}(\mathbb{F}_2)$, 其中 k 为奇数. 假设 $a_{ij} + a_{ji} = 1$ 对任意 $i \neq j$ 都成立, 且 $\sum_j a_{ij} = 0, \forall i$. 令 $A' = (a'_{ij}) \in M_{k \times k}(\mathbb{F}_2)$ 满足 $a'_{ij} = a_{ij}$, 若 $i \neq j$; $a'_{ii} = a_{ii} + 1, \forall i$, 则有 $\text{rank} A' = \text{rank} A + 1$.

命题 4.1 令 $n \equiv -1 \pmod{24}$ 为一个平方自由的正整数且其所有素因子都满足模 24 余 ± 1 , 则 $\mathbb{Q}(\sqrt{-n})$ 没有 4 阶元当且仅当 $\text{Sel}_2(E^{(\pm n)}/\mathbb{Q})/E^{(\pm n)}[2] = 1$.

证明 令 $m = \pm n$, 注意到 m 对应的矩阵 A 为 $\mathbb{Q}(\sqrt{-n})$ 对应的 Rédei 矩阵, 故条件 $\mathbb{Q}(\sqrt{-n})$ 没有 4 阶元等价于 A 的余秩为 1 (因此由前述引理可知 $A + D_{-1}$ 为非退化矩阵).

首先假设 $m > 0$. 若 C_Λ 在 6∞ 处有解, 则 $(2, b_1 b_2) = 1, (\frac{b_2}{3}) = 1$ 且 $b_1 b_2 > 0$. 可能的使得 C_Λ 在所有整除 6∞ 的素数处都有解的 (c_1, c_2) 为 $(1, 1), (3, 1), (-1, -1), (-3, -1)$.

更进一步地, $(b_1, b_2) = (3, 1)$ 总是 C_Λ 的一个关于所有 $\mathbb{Q}_p$ 的解, 且它不是来自挠点.

假设 $m < 0$, 若 C_Λ 在 $p \mid 6\infty$ 处有解, 则 $(b_1, 2) = 1, (3, b_2) = 1$, 且若 $3 \nmid b_1$, 则 $\frac{b_2}{3} = 1$ 成立; 若 $3 \mid b_1$, 则 $(\frac{b_2}{3}) = -1$ 成立. 唯一可能的使得 C_Λ 在整除 6∞ 的素数处都有解的 (c_1, c_2) 由以下条件给出:

$$(1, 1), (-1, 1), (3, 1), (-3, 1), (1, 2), (-1, 2), (3, 2), (-3, 2).$$

更进一步地, $(b_1, b_2) = (3, 2)$ 总是 C_Λ 关于所有 $\mathbb{Q}_p$ 的解, 且它不是来自于挠点.

当 $\text{Cl}(\mathbb{Q}(\sqrt{-d}))$ 没有 4 阶元时,

$$\begin{pmatrix} A & D_{-3} \\ & A + D_{-1} \end{pmatrix} \quad \text{和} \quad \begin{pmatrix} A + D_{-1} & D_{-3} \\ & A \end{pmatrix}$$

的余秩都为 1. 若 $m > 0$, 则 2-Selmer 秩为 3 且所有的解 (b_1, b_2) 为

$$(1, 1), (m, 1), (3, 1), (3m, 1), (-m, -m), (-1, -m), (-3m, -m), (-3, -m).$$

若 $m < 0$, 由 3-进局部条件可知对每个 (c_1, c_2) , 只有一个 (b_1, b_2) 满足每个局部都有解, 则 2-Selmer 秩为 3 且所有的解 (b_1, b_2) 为

$$(1, 1), (m, 1), (-3m, -m), (-3, -m), (-m, -2m), (-1, -2m), (3, 2), (3m, 2).$$

另一方面, 若 $\text{Cl}(\mathbb{Q}(\sqrt{-d}))$ 有一个 4 阶元, 当 $m > 0$ 时, 取 (c_1, c_2) 为 $(3, 1)$; 当 $m < 0$ 时, 取 (c_1, c_2) 为 $(3, 2)$, 则

$$\begin{pmatrix} A & D_{-3} \\ & A + D_{-1} \end{pmatrix} \quad \text{和} \quad \begin{pmatrix} A + D_{-1} & D_{-3} \\ & A \end{pmatrix}$$

的余秩都比 2 大, 故有 2-Selmer 秩至少为 4. □

用类似的方法可以证明:

命题 4.2 令 $m \equiv 1 \pmod{24}$ 为一个平方自由的正整数, 则

$$\text{rank}_{\mathbb{F}_2} \text{Sel}_2((E^{(-m)}/\mathbb{Q})) > \text{rank}_{\mathbb{F}_2}(E^{(-m)}(\mathbb{Q})[2]).$$

4.2 2-部分 BSD 公式

令 $E/\mathbb{Q}$ 为椭圆曲线 $y^2 = x(x-1)(x+3)$. 令 $n \equiv -1 \pmod{24}$ 满足其所有素因子模 24 余 ± 1 . 令 $D = -n$.

定理 4.1 若 $\text{Cl}(\mathbb{Q}(\sqrt{-n}))$ 没有 4 阶元, 则 $E^{(-\epsilon n)}$ 的代数秩和解析秩都为 1, 其代数 Sha 群的阶 $\#\text{III}(E^{(-\epsilon n)})$ 和解析 Sha $\mathcal{L}'(E^{(-\epsilon n)})$ 都为奇数, 即 $E^{(-\epsilon n)}$ 的 2-部分 BSD 公式成立.

证明 由 Gross-Zagier 公式和定理 3.1, 可知秩部分成立. 由 Kolyvagin 的结果知, Sha 群有限. 更进一步地, 由上一小节的 2 递降可知 Sha 群的阶为奇数. 故 BSD 公式 2-部分归结到证明解析 Sha 为奇数, 这可由精确 Gross-Zagier 公式和 Heegner 点的 2 可除性得到. 令 $A = E^{(\epsilon)}$, $K = \mathbb{Q}(\sqrt{-n})$, y_K 为 $(A, \mathbf{1}_K)$ 对应的 Heegner 点. 回顾精确 Gross-Zagier 公式为

$$L(1, A)L(1, A^{(-n)}) = \frac{8\pi^2(\phi, \phi)}{\sqrt{n}} \frac{\hat{h}_K(y_K)}{\deg f},$$

其中

$$\deg(f) = \begin{cases} 1, & \text{若 } \epsilon = 1, \\ 2, & \text{若 } \epsilon = -1. \end{cases}$$

注意到

$$L^{\text{alg}}(1, A) = \begin{cases} \frac{1}{8}, & \text{若 } \epsilon = 1, \\ \frac{1}{4}, & \text{若 } \epsilon = -1, \end{cases}$$

$$8\pi^2(\phi, \phi) = \begin{cases} \frac{1}{2}\Omega(A)\Omega(A^{-1}), & \text{若 } \epsilon = 1, \\ \Omega(A)\Omega(A^{-1}), & \text{若 } \epsilon = -1, \end{cases}$$

且由文献 [22] 可知

$$\Omega(A^{(-n)}) = \frac{\Omega(A^{(-1)})}{\sqrt{n}},$$

故有

$$\frac{L'(1, A^{(-n)})}{\Omega(A^{(-n)})} = \begin{cases} 4\hat{h}_K(y_K), & \text{若 } \epsilon = 1, \\ 2\hat{h}_K(y_K), & \text{若 } \epsilon = -1. \end{cases}$$

令 y 为 $A^{(-n)}(\mathbb{Q})$ 的一个生成元, 则由定理 3.1 中 Heegner 点的 2 可除性可知等式

$$\hat{h}_K(y_K) = a \cdot 2^{2k-3} \hat{h}_{\mathbb{Q}}(y)$$

对某个奇数 a 成立. 由 Tate 的算法 [23] 可知,

$$c_2(A) = \begin{cases} 4, & \text{若 } \epsilon = 1, \\ 2, & \text{若 } \epsilon = -1, \end{cases} \quad c_3(A) = 2, \quad c_p(A) = 4 \quad \text{若 } p \mid n, \quad (p, 24) = 1,$$

故

$$\mathcal{L}'(A^{(-n)}) = \frac{L'(1, A^{(-n)})}{\Omega(A^{(-n)})\hat{h}_{\mathbb{Q}}(y)} \cdot \frac{\#(A^{(-n)}(\mathbb{Q})_{\text{tor}})^2}{\prod_{\ell} c_{\ell}(A^{(-n)})}$$

为一个奇数. □

参考文献

- 1 Besson M. Tiling a triangle with congruent triangles. <http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.180.4908>, 2010
- 2 Fujiwara M. θ -congruent numbers. In: Number Theory. Berlin: de Gruyter, 1998, 235–241
- 3 Laczkovich M. Rational points of some elliptic curves related to the tilings of the equilateral triangle. Discrete Comput Geom, 2020, 64: 985–994
- 4 Qin H R. Congruent numbers, quadratic forms and K_2 . Math Ann, in press, 2021
- 5 Yoshida S. Some variants of the congruent number problem II. Kyushu J Math, 2002, 56: 147–165
- 6 Yoshida S. Some variants of the congruent number problem I. Kyushu J Math, 2001, 55: 387–404
- 7 Kan M. θ -congruent numbers and elliptic curves. Acta Arith, 2000, 94: 153–160
- 8 Tian Y. Congruent numbers and Heegner points. Camb J Math, 2014, 2: 117–161
- 9 Tian Y, Yuan X Y, Zhang S W. Genus periods, genus points and congruent number problem. Asian J Math, 2017, 21: 721–774
- 10 Smith A. 2^∞ -Selmer groups, 2^∞ -class groups, and Goldfeld's conjecture. arXiv:1702.02325, 2017
- 11 Bhargava M, Kane D M, Lenstra H W, et al. Modeling the distribution of ranks, Selmer groups, and Shafarevich-Tate groups of elliptic curves. Camb J Math, 2015, 3: 275–321
- 12 Yuan X Y, Zhang S W, Zhang W. The Gross-Zagier Formula on Shimura Curves. Annals of Mathematics Studies, vol. 184. Princeton: Princeton University Press, 2013
- 13 Kolyvagin V A. On the structure of Shafarevich-Tate groups. In: Algebraic Geometry. Lecture Notes in Mathematics, vol. 1479. Berlin-Heidelberg: Springer, 1989, 94–121
- 14 Cai L, Shu J, Tian Y. Explicit Gross-Zagier and Waldspurger formulae. Algebra Number Theory, 2014, 8: 2523–2572
- 15 Cai L, Li C, Zhai S. On the 2-part of the Birch and Swinnerton-Dyer conjecture for quadratic twists of elliptic curves. J Lond Math Soc (2), 2020, 101: 714–734
- 16 Xue J, Yang T C, Yu C F. Supersingular abelian surfaces and Eichler's class number formula. Asian J Math, 2019, 23: 651–680
- 17 Coates J, Li Y, Tian Y, et al. Quadratic twists of elliptic curves. Proc Lond Math Soc (3), 2015, 110: 357–394

- 18 Gross B. Heegner points on $X_0(N)$. In: Modular Forms. Ellis Horwood Series in Mathematics and its Applications: Statistics and Operations Research. Chichester: Horwood, 1984, 87–105
- 19 Ligozat G. Courbes modulaires de genre 1. Bull Soc Math France, 1964, 1: 5–80
- 20 Agashe A, Stein W. Visible evidence for the Birch and Swinnerton-Dyer conjecture for modular abelian varieties of analytic rank zero. Math Comp, 2005, 74: 455–484
- 21 Cai L, Li Y X, Wang Z J. Special automorphisms on Shimura curves and non-triviality of Heegner points. Sci China Math, 2016, 59: 1307–1326
- 22 Pal V. Periods of quadratic twists of elliptic curves. Proc Amer Math Soc, 2012, 140: 1513–1525
- 23 Silverman H. Advanced Topics in the Arithmetic of Elliptic Curves. New York: Springer-Verlag, 1994

Tiling number problem and θ -congruent number problem

Wei He, Yirong Hu & Ye Tian

Abstract The tiling number problem is closely related to the arithmetic of elliptic curves. In this paper, we construct a family of tiling numbers with multiple prime factors by using Birch lemma and the induction method developed by one of the authors (Ye Tian) to prove the non-torsionness of Heegner points. In addition, we prove the 2-part BSD conjecture of the related elliptic curves. We deal with the quadratic twist family of elliptic curves without complex multiplication and the distribution of 2-Selmer groups of this family is not predicted by the general conjecture or the known results.

Keywords tiling number, elliptic curve, BSD conjecture, Waldspurger formula, Gross-Zagier formula

MSC(2020) 11G40, 11G05, 11D25

doi: 10.1360/SSM-2020-0354