中国科学技术大学

博士学位论文

椭圆曲线的二次扭系列

作者姓名：张神星

学科专业：基础数学

导师姓名：欧阳毅　教授

完成时间：二〇一五年九月

University of Science and Technology of China

A dissertation for doctor's degree

Some series of quadratic twists of elliptic curves

Author :	Shenxing Zhang
Speciality :	Pure Mathematics
Supervisor :	Prof. Yi Ouyang
Finished Time :	September, 2015

中国科学技术大学学位论文原创性声明

本人声明所呈交的学位论文，是本人在导师指导下进行研究工作所取得的成果。除已特别加以标注和致谢的地方外，论文中不包含任何他人已经发表或撰写过的研究成果。与我一同工作的同志对本研究所做的贡献均已在论文中作了明确的说明。

作者签名：_____　　签字日期：_____

中国科学技术大学学位论文授权使用声明

作为申请学位的条件之一，学位论文著作权拥有者授权中国科学技术大学拥有学位论文的部分使用权，即：学校有权按有关规定向国家有关部门或机构送交论文的复印件和电子版，允许论文被查阅和借阅，可以将学位论文编入《中国学位论文全文数据库》等有关数据库进行检索，可以采用影印、缩印或扫描等复制手段保存、汇编学位论文。本人提交的电子文档的内容和纸质论文的内容相一致。

保密的学位论文在解密后也遵守此规定。

☐ 公开　☐ 保密 _____ 年

作者签名：_____　　导师签名：_____

签字日期：_____　　签字日期：_____

摘　要

本文研究了几类椭圆曲线的二次扭系列. 具体来说, 我们研究了同余数曲线的二次扭系列, 并构造了一系列秩零的二次扭; 研究了函数域上椭圆曲线的二次扭系列, 并构造了一系列秩一的二次扭.

在第一章中, 我们回顾了 BSD 猜想和同余数的历史和进展, 并陈述了我们的主要结果.

在第二章中, 我们回顾了椭圆曲线的基本理论和本文需要使用的主要概念.

在第三章中我们给出了三个不同系列的非同余数的一个充分性判断条件. 前三节我们介绍了同余数的概念, 并引入了基本的记号, 陈述了主要结论, 介绍了证明策略和方法. 我们的主要策略是对同余椭圆曲线次数为 2 的同源的 Selmer 像的大小进行估计, 以此来保证弱 Mordell–Weil 群达到极小. 这种做法可以在弱 Mordell–Weil 群达到极小的情形下, 得到 Tate–Shafarevich 群 2 部分不平凡的同余椭圆曲线. 4-7 节对 Selmer 群进行了具体的计算和判断, 并在最后一节完成了主要结论的证明.

在第四章中，我们首先简单介绍了函数域上椭圆曲线的模性和模曲线, 给出了数域情形的 Birch 引理在函数域上的类比. 通过研究椭圆曲线上 Heegner 点上的作用, 导出了 Heegner 点的无挠性, 并得到了一系列秩一的椭圆曲线.

我们在论文最后给了一点展望.

关键词： 椭圆曲线, 非同余数, 2 下降法, Birch 引理, Heegner 点

ABSTRACT

In this paper, we study several series of quadratic twists of elliptic curves. We construct several series of congruent elliptic curves with rank zero and elliptic curves over function fields with rank one.

In Chapter 1, we recall the history of BSD conjecture and the congruent number problem, and state our main results.

In Chapter 2, we recall basic theory and notations on elliptic curves.

In Chapter 3, we give three different series of non-congruent numbers. In Section 1-3, we introduce the definition of congruent numbers and basic notations, state main result and give our strategy. We estimate the image of the Selmer groups of isogenies of degree 2, to ensure the weak Mordell–Weil group is minimal. Then we can obtain congruent elliptic curves with non-trivial Tate–Shafarevich group. In Section 4-8, we calculate the Selmer groups and finish the proof.

In Chapter 4, we introduce the modularity of elliptic curves over function fields and modular curves. We give a function field version of Birch lemma. We study the Heegner points and prove it is non-torsion, then we obtain several series of elliptic curves with rank one.

We give some perspective at the last chapter.

Keywords: Elliptic curve, non-congruent number, 2-descent, Birch lemma, Heegner point

常用记号

$\mathbb{Z}$	整数环
$\mathbb{Q}$	有理数域
p	素数
$\mathbb{F}_q$	q 元有限域
F, K	域
Pic	理想类群, Picard 群
h, h_F, h_K	类数
$v, \mathfrak{p}, \mathfrak{q}, \mathfrak{q}_i$	素位, 素理想
$H_{\mathfrak{q}}, H_{\mathfrak{q}_i}, H_{\mathfrak{d}}, H_{\mathfrak{M}}$	环类域
F_v	F 在 v 处的完备化
$\kappa(v)$	v 处的剩余域
$\mathcal{O}$	离散赋值环的整数环, 整体域的整数环, 序模
Gal	Galois 群
Tr	迹
Re	复数的实部
$\sqrt{-1}, i, i'$	-1 的平方根
τ, μ	$d = \tau^2 - b_1\mu^2$ 的解
(a, b)	最大公因子
v, v_p	规范赋值, $v_p(p) = 1$
$O(x)$	赋值不小于 x 的赋值的数
$\left(\frac{x}{p}\right)$	Legendre 符号
$\left(\frac{x}{m}\right)$	Jacobi 符号
$\left[\frac{x}{p}\right]$	加性 Legendre 符号
$\left[\frac{x}{m}\right]$	加性 Jacobi 符号
A, C	$\mathbb{F}_2$ 上矩阵
$\overrightarrow{x}$	$\mathbb{F}_2$ 上向量
$\overrightarrow{0}$	$\mathbb{F}_2$ 上分量全为 0 的向量
$\overrightarrow{1}$	$\mathbb{F}_2$ 上分量全为 1 的向量
$d(\overrightarrow{x})$	$\overrightarrow{x}$ 非零分量对应素元之积
$\overrightarrow{d}$	d 因子对应非零分量的向量
rank	有限生成阿贝尔群的秩, 矩阵的秩
ord	函数在一点处的阶

dim	维数
(E, O)	椭圆曲线
$\mathbb{P}^n$	n 维射影空间
$X_0(N)$	模曲线
E_{tor}	E 的有限阶元
E_1, E_2, E_3, E_i	同余椭圆曲线
E_1', E_2', E_3', E_i'	同余椭圆曲线的对偶
$E^{(n)}$	二次扭
$\tilde{E}$	E 在剩余域的约化
a_v, a_n	Fourier 系数
$L(E, s)$	L 函数
$\Gamma(s)$	Γ 函数
ϕ, φ, ψ	同源
$[\phi], [2], [2^\infty]$	被零化的部分
$[m]$	m 倍映射
Sel	Selmer 群
$\widetilde{\text{Sel}}$	Selmer 群的像
Ш	Ш 群, Tate–Shafarevich 群
C_d, C_d'	齐性空间
$\mathcal{M}_s$	见(3.8),(3.13)
$X_0(N)$	模曲线
T_n	Hecke 算子
$w_{\mathfrak{p}}, w_N$	Atkin–Lehner 算子
P_0	O 的原像
$P_{\mathfrak{a},\mathfrak{N},\mathfrak{M}}, P_{\mathfrak{M}}$	Heegner 点
χ	χ 部分
$^-$	$\tau = -1$ 部分

目 录

第一章　绪论

本章分为三节, 分别介绍论文的研究背景, 主要结果以及证明策略.

1.1　研究背景

1.1.1　椭圆曲线和 BSD 猜想

数论中一个经典分支是关于 Diophantine 方程的解. 对于线性方程和二次曲线, 容易从一个解出发得到所有的解. 对于整体域 F 上亏格大于 1 的曲线 C, Faltings [Fal] 于 1983 年证明了著名的 Mordell 猜想 (后称为 Faltings 定理), 即曲线 C 的 F 点只有有限多个. 而对于亏格为 1 的光滑曲线, 即椭圆曲线, 其上的 F 点形成了一个阿贝尔群, 称为 **Mordell–Weil 群**. 这个群的算术信息和它对应的 L 函数有着深刻的联系, 这种联系在 20 世纪 60 年代由 Birch 和 Swinnerton-Dyer 以猜想的方式提出, 即著名的 BSD 猜想 [BSD]. 它断言 Mordell–Weil 群的秩和 $L(E,s)$ 在 $s=1$ 处的阶相等. 该猜想于 2000 年被 Clay 数学研究所列入千禧年七大数学难题, 并悬赏 100 万美元奖励给第一个给出证明的人.

1977 年, Coates 和 Wiles [CoW] 首次在该问题上取得突破. 他们证明了如果椭圆曲线 E 带类数为 1 的复乘域 K 且 E 定义在域 $F=K$ 或有理数域 $F=\mathbb{Q}$ 上, 则 $L(E,1)=0$ 蕴含 $E(F)$ 有限. Arthaud [Art] 于 1978 年证明可将 F 替换为 K 的任意有限 Abel 扩张.

Langlands 猜想认为 $L(E,s)$ 等于某个自守形式的 L 函数, 从而可以解析延拓至整个复平面, 这种性质称为**模性**. 1986 年, Gross 和 Zagier [GrZ] 证明了如果椭圆曲线有模性, 则 $L(E,s)$ 在 $s=1$ 处阶恰好为 1 蕴含 E 包含无限阶有理点. 由此, Kolyvagin [Kol] 于 1989 年证明了具有模性的椭圆曲线在 $L(E,s)$ 在 $s=1$ 的阶 ≤ 1 时, BSD 猜想成立.

BSD 猜想还断言 $L(E,s)$ 在 $s=1$ 处的 Taylor 展开的首项系数与 E 的 Tate–Shafarevich 群大小, Mordell–Weil 群有限部分大小, 单元基准, 玉河数有着精确的等式联系. 这部分通常被称作精确 BSD 猜想, 相应地, 前者则被称作弱 BSD 猜想. 由于我们已经知道精确 BSD 猜想两边都是 F 中元素, 所以只需证明它们在每个素位相等即可.

Rubin [Rub2] 于 1991 年证明了对于带复乘 K 且定义在 K 上的椭圆曲线 E, 如果 $L(E,1)$ 非零, 则精确 BSD 猜想的 $p>7$ 部分均相等.

Wiles, Breuil, Conrad, Diamond 和 Taylor [Wil, BCDT] 证明了有理数域 $\mathbb{Q}$ 上的椭圆曲线的模性. Deligne, Drinfeld 和 Zarhin 证明了函数域上的椭圆曲线的模

性. 而函数域的 BSD 猜想, 根据 Tate, Milne, Kato 和 Trihan 等人的工作, 只需证明 Tate–Shafarevich 群的任一 p 部分有限即可推出精确 BSD 成立.

1.1.2　同余数

阿拉伯人 Mohammed Ben Alhocain 在一份 10 世纪的手稿中提出了一个问题: 何时 n 能成为由 3 个平方数构成的等差数列的公差 (见 [Dic, 第 16 章])? 这等价于 n 是同余数. 我们利用同余椭圆曲线的 L 函数的函数方程可以知道 $n \equiv 5, 6, 7 \bmod 8$ 时, 其 L 函数在 $s = 1$ 处的阶为奇数, 如果 BSD 猜想成立, 则 n 是同余数.

在同余数方面, Heegner [Hee] 证明了 $p \equiv 5, 7$ 或 $2p \equiv 6 \bmod 8$ 是同余数, 其中 p 是素数. 田野 [Tia] 证明了对任意正整数 k, 存在无穷多个同余数恰好有 k 个素因子.

非同余数方面, Fermat 证明了 1 和 2 是非同余数, 其证明本质上是 2 下降法. 冯克勤 [冯] 利用 2 下降法证明了对任意正整数 k, 存在无穷多个 Tate–Shafarevich 群 2 部分平凡的非同余数恰好有 k 个素因子, 而根据 Monsky 的结果可以完全确定所有 Tate–Shafarevich 群 2 部分平凡的非同余数, 参见 [HeB]. 李德琅和田野 [LiT] 利用二阶 2 下降法对 Selmer 群进行了进一步的估计并找到了一系列 Tate–Shafarevich 群 2 部分大小为 4 的非同余数.

1.2　主要结果

在第三章中, 我们利用了二阶 2 下降法找到了一系列 Tate–Shafarevich 群 2 部分大小为 4 的非同余数. 对于无平方因子的正整数 n, 我们定义了矩阵 A, C_a, 参见 §3.2. 我们的主要结果为:

定理 1.2.1. (1) 设 $n \equiv 1 \bmod 8$, $p_i \equiv 1 \bmod 4$, $\operatorname{rank} A = k - 1$. 设 $\overrightarrow{v}$ 是方程 $A\overrightarrow{x} = C_2\overrightarrow{1}$ 的一个根, 令 $d = d(\overrightarrow{v})$. 令 $2d = \tau^2 + \mu^2$, 选取 $\sqrt{-1} \in \mathbb{Z}/n\mathbb{Z}$ 使得对任意 $p \mid d$, $p \mid \tau - \sqrt{-1}\mu$. 若 $\left(\frac{\tau+\sqrt{-1}\mu}{n}\right)\left(\frac{2}{d}\right) = -1$, 则 n 是非同余数.

特别地, 如果 $p_i \equiv 1 \bmod 8$, $\operatorname{rank} A = k - 1$, $\left(\frac{1+\sqrt{-1}}{n}\right) = -1$, 则 n 是非同余数.

(2) 设 $m \equiv 1 \bmod 8$, $p_i \equiv \pm 1 \bmod 8$, $\operatorname{rank} A = \operatorname{rank}(A + C_{-1}) = k - 1$. 令 $m = 2\mu^2 - \tau^2$. 若 $|\mu| \equiv 3 \bmod 4$, 则 $n = m$ 是非同余数. 若 $\left(\frac{2+\sqrt{2}}{m}\right) = -1$, 则 $n = 2m$ 是非同余数.

(3) 令 n 为 (1) 或 (2) 中的 n, $E : ny^2 = x^3 - x$, 则

$$\operatorname{rank} E(\mathbb{Q}) = 0, \quad Ш(E/\mathbb{Q})[2^\infty] \cong (\mathbb{Z}/2\mathbb{Z})^2. \tag{1.1}$$

在第四章中, 如果函数域 F 及其上的有限素位 $\mathfrak{q}_i$ 和虚二次扩张 $K = F(\sqrt{l})$ 满足我们给定的假设 (I)-(V), 令 τ 为 $\operatorname{Gal}(K_\infty/F_\infty)$ 中非平凡元素, 则我们有:

定理 1.2.2. 设 $\mathfrak{M} = \prod_{i=1}^{r} \mathfrak{q}_i$, h 是 F 在无穷素位 ∞ 的类数, M_0 是 $\mathfrak{M}^h$ 的一个生成元使得 M_0 的像是 F 在 ∞ 的剩余域中的平方, $M = M_0$ 或 lM_0 使得 $\tau(\sqrt{M}) = -\sqrt{M}$. 则 E 关于 M 的二次扭 $E^{(M)}$ 秩为 1 且精确 *BSD* 猜想成立.

1.3　证明策略

在第三章中, 我们将利用二阶 2 下降法对同余椭圆曲线 E_i 的同源对应的 Selmer 群进行计算和估计, 由此估计出弱 Mordell–Weil 群的大小.

在第四章中, 我们将说明 E 上 Heegner 点构成 Euler 系, 利用我们的假设条件构造出 E 的无限阶有理点. 最后证明 Tate–Shafarevich 群的有限性, 并由此得到 BSD 猜想.

第二章　椭圆曲线的一般理论

本章我们将回顾椭圆曲线的基本知识. 我们假设读者具有代数几何的基本知识, 相关文献可以参考 [Har, Sil].

2.1 Weierstrass 方程

设 F 是域. 称 (E, O) 为 F 上的**椭圆曲线**, 如果 E 是 F 上亏格为 1 的光滑曲线, O 是 E 的一个 F 点.

命题 2.1.1. *E 可以写成 $\mathbb{P}^2_F$ 上的一条三次曲线*

$$Y^2 + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3,\ a_i \in F \tag{2.1}$$

使得 $O = [0, 1, 0]$.

证明. 参见 [Sil, III §3]. 令

$$\mathcal{L}(n(O)) = \{f \in \bar{F}(E)^\times : \mathrm{div}(f) \geq -n(O)\} \cup \{0\}.$$

由 Riemann–Roch 定理 ([Sil, II 定理 5.4, 推论 5.5]), $\dim \mathcal{L}(n(O)) = n$. 因此我们可以选取 $x, y \in F(E)$ 使得 $\{1, x\}$ 为 $\mathcal{L}(2(O))$ 的一组基, $\{1, x, y\}$ 为 $\mathcal{L}(3(O))$ 的一组基. 注意到 $\dim \mathcal{L}(6(O)) = 6$, 而

$$1, x, y, x^2, xy, y^2, x^3$$

均落在该空间, 因此它们线性相关

$$A_1 + A_2x + A_3y + A_4x^2 + A_5xy + A_6y^2 + A_7x^3 = 0, \quad A_i \in F.$$

注意到 x 和 y 在 O 的阶为 -2 和 -3, 因此 $A_6A_7 \neq 0$. 将 x 和 y 分别替换为 $-A_6A_7x$ 和 $A_6A_7^2y$, 则我们得到方程 (2.1). 从而

$$\phi = [x, y, 1] : E \to \mathbb{P}^2$$

给出满射 $\phi : E \to C = \mathrm{im}(E)$. 注意到 x 和 y 仅在 O 处有极点, 因此

$$[K(E) : K(x)] = 2, [K(E) : K(y)] = 3,$$

从而 $K(E) = K(x, y)$.

若 C 奇异, 则存在次数为 1 的有理映射 $\psi : C \to \mathbb{P}^1$, 从而 $\psi \circ \phi : E \to \mathbb{P}^1$ 是同构, 这不可能. 因此 C 是光滑曲线, ϕ 是同构. □

方程 (2.1) 被称为 E 的 **Weierstrass 方程**, 它的非齐次形式为

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6. \tag{2.2}$$

如果 F 的特征不为 2, 则 (2.2) 可以变为如下形式:

$$y^2 = x^3 + ax^2 + bx + c. \tag{2.3}$$

如果 F 的特征不为 2 和 3, 则 (2.2) 可以变为如下形式:

$$y^2 = x^3 + bx + c. \tag{2.4}$$

2.2　群结构

设 $E \subset \mathbb{P}_F^2$ 是一条椭圆曲线, P, Q 是 E 上的两个点. 根据相交理论, 过 P, Q 的直线 $L \subset \mathbb{P}^2$ 交 E 于 P, Q 及另一点 R, 过 R, O 的直线 L' 交 E 于 R, O 及另一点 R', 我们定义 $P + Q = R'$. 这里交点需计算重数.

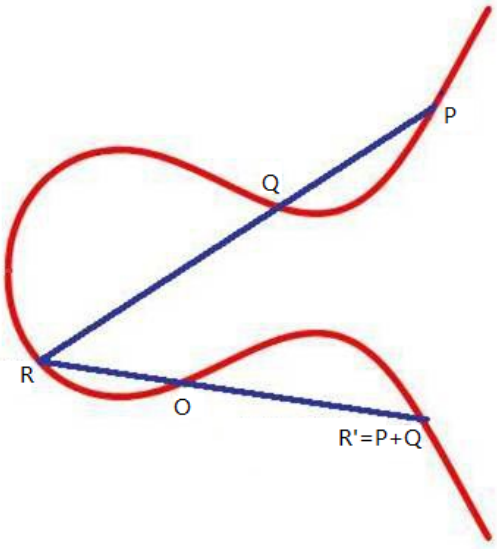

图 2.1　椭圆曲线的加法

利用 E 的 Weierstrass 方程, 我们可以具体地写出加法的坐标形式, 并由此可以得到:

命题 2.2.1. $(E, O, +)$ 构成阿贝尔群.

注 2.2.2. 定义 $P +_{O'} Q := P + Q - O'$, 则 $(E, O', +_{O'})$ 构成一个阿贝尔群. 由此可知我们可以选择 E 上任何一个点作为群结构的零元.

设 E 的 Weierstrass 方程为 (2.3), $P = (x_1, y_1)$, 则利用 Viète 定理可知 $2P = (x_2, y_2)$, 其中

$$\begin{aligned} x_2 =& \frac{1}{4y_1^2}(x_1^4 - 2bx_1^2 - 8cx_1 + b^2 - 4ac, \\ y_2 =& \frac{1}{8y_1^3}(x_1^6 + 2ax_1^5 + 5bx_1^4 + 20cx_1^3 + (20ac - 5b^2)x_1^2 \\ &+ (8a^2c - 2ab^2 - 4bc)x_1 + (4abc - 8c^2 - b^3)). \end{aligned} \tag{2.5}$$

2.3　同源

定义 2.3.1. 设 $\phi : (E, O) \to (E', O')$ 是椭圆曲线的态射. 如果 ϕ 不是常数且 $\phi(O) = O'$, 称 ϕ 是一个**非零同源**, 此时亦称 E 与 E' **同源**.

命题 2.3.2. 设 $\phi : E \to E'$ 是一个可分的非零同源.

(1) ϕ 是满同态.

(2) $\ker\phi$ 有限且等于态射 ϕ 的次数.

(3) 设 $m = \#\ker\phi$. 存在唯一的同源 $\hat{\phi} : E' \to E$, 使得 $\hat{\phi} \circ \phi = [m]$ 是 m 倍映射, 且有 $\hat{\hat{\phi}} = \phi$.

证明. 参见 [Sil, III 定理 4.3, 6.1, 6.2]. □

$\hat{\phi}$ 称为 ϕ 的**对偶**.

2.4　二次扭

假设域 F 的特征不为 2, $n \in F - F^2$. 若椭圆曲线 E/F 的 Weierstrass 方程为 (2.3), 则 E 关于 n 的**二次扭** $E^{(n)}$ 为

$$ny^2 = x^3 + ax^2 + bx + c.$$

这同构于

$$y^2 = x^3 + anx^2 + bn^2x + cn^3.$$

命题 2.4.1. 设 $K = F(\sqrt{n})$ 为 F 的二次扩张, $\tau \in \mathrm{Gal}(K/F)$ 将 $\sqrt{n}$ 映为 $-\sqrt{n}$, 则 $E(K)^- \cong E^{(n)}(F)$, 这里 $^-$ 表示 $\tau = -1$ 的部分.

证明. 定义

$$\varphi : E^{(n)}(F) \to E(K)^-, \quad (x, y) \mapsto (x, \sqrt{n}y).$$

容易验证 φ 是群的单同态. 若 $(x, y) \in E(K)^-$, 则

$$\tau(x, y) = (\tau x, \tau y) = -(x, y) = (x, -y),$$

故 $x \in F, y \in F^-, y/\sqrt{n} \in F$, $\varphi(x, y/\sqrt{n}) = (x, y)$. 因此 φ 是群同构. □

2.5　Mordell 定理

以下设 F 为整体域, 即 F 是有理数域 $\mathbb{Q}$ 或有理函数域 $\mathbb{F}_p(t)$ 的有限扩张.

定理 2.5.1 (Mordell)**.** $E(F)$ 是有限生成阿贝尔群.

证明. 参见 [Sil, VIII §6]. □

Weil 将 Mordell 定理推广至一般的阿贝尔簇也成立.

2.6　Selmer 群和 Tate–Shafarevich 群

定义 2.6.1. 设 $\phi : E \to E'$ 是 F 上椭圆曲线的一个同源. 定义 ϕ-*Selmer* 群为

$$\mathrm{Sel}^{(\phi)}(E/F) = \ker\{\mathrm{H}^1(F, E[\phi]) \to \prod_v \mathrm{H}^1(F_v, E)\},$$

定义 *Tate–Shafarevich* 群为

$$Ш(E/F) = \ker\{\mathrm{H}^1(F, E) \to \prod_v \mathrm{H}^1(F_v, E)\},$$

其中 v 取遍 F 所有的素位.

命题 2.6.2. 我们有基本正合列

$$0 \to E'(F)/\phi(E(F)) \to \mathrm{Sel}^{(\phi)}(E/F) \to Ш(E/F)[\phi] \to 0, \tag{2.6}$$

其中 $[\phi]$ 表示被 ϕ 零化的部分.

证明. 我们对正合列

$$0 \to E[\phi] \to E \to E' \to 0,$$

取 $\mathrm{Gal}(\bar{F}/F)$ 和 $\mathrm{Gal}(\bar{F}_v/F_v)$ 模上同调得到长正合列

$$0 \to E(F)[\phi] \to E(F) \to E'(F) \to \mathrm{H}^1(F, E[\phi]) \to \mathrm{H}^1(F, E) \to \mathrm{H}^1(F, E'),$$

$$0 \to E(F_v)[\phi] \to E(F_v) \to E'(F_v) \to \mathrm{H}^1(F_v, E[\phi]) \to \mathrm{H}^1(F_v, E) \to \mathrm{H}^1(F_v, E'),$$

由此我们有

$$\begin{array}{ccccccccc}
0 & \longrightarrow & E'(F)/\phi E(F) & \longrightarrow & \mathrm{H}^1(F, E[\phi]) & \longrightarrow & \mathrm{H}^1(F, E)[\phi] & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & \prod_v E'(F_v)/\phi E(F_v) & \longrightarrow & \prod_v \mathrm{H}^1(F_v, E[\phi]) & \longrightarrow & \prod_v \mathrm{H}^1(F_v, E)[\phi] & \longrightarrow & 0.
\end{array}$$

利用图表追踪法可得正合列 (2.6), 参见 [Sil, 333 页]. □

2.7　齐性空间

本节内容参见 [Sil, X §4 例子 4.8]. 令 $F = \mathbb{Q}$, $\phi : E \to E'$ 是次数为 2 的同源, 其中

$$E : y^2 = x^3 + ax^2 + bx,$$

$$E' : y^2 = x^3 - 2ax^2 + (a^2 - 4b)x.$$

设 $v = v_p$ 表示规范的 p 进赋值, 即 $v(p) = 1$. 令

$$S = \{\infty, p \mid 2b(a^2 - 4b)\},$$

$$\mathbb{Q}(S,2) := \{b \in \mathbb{Q}^\times/\mathbb{Q}^{\times 2} : \text{对任意} p \notin S, v_p(b) \text{是偶数}\}.$$

$2b(a^2-4b)$ 所有无平方因子的约数可以代表整个集合 $\mathbb{Q}(S,2)$, 我们将不加区分地使用它们. 令 C_d 是 $d \in \mathbb{Q}(S,2)$ 对应的 E 的**齐性空间**:

$$C_d : dw^2 = d^2 - 2adz^2 + (a^2-4b)z^4.$$

引理 2.7.1. *Selmer 群* $\mathrm{Sel}^{(\phi)}(E/\mathbb{Q})$ *可以等同于*

$$\mathrm{Sel}^{(\phi)}(E/\mathbb{Q}) = \{d \in \mathbb{Q}(S,2) : \text{对任意} v \in S, C_d(\mathbb{Q}_v) \text{非空}\}.$$

证明. 参见 [Sil, X §4]. □

由此可知, Selmer 群的计算可以化为解局部域上的方程, 而这很容易利用 Hensel 引理来解答.

2.8　约化和 L 函数

记 F 在 v 的完备化为 F_v, $\mathcal{O}_v$ 为 F_v 的整数环, $\kappa(v)$ 为 O_v 的剩余域.

命题 2.8.1. *在* E/F_v *所有的系数落在* $\mathcal{O}_v$ *的 Weierstrass 方程中, 存在一个判别式的赋值达到最小的方程.*

证明. 参见 [Rub, §3.1]. □

我们称其为**极小 Weierstrass 方程**, 不妨仍记作

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

我们将系数 a_i 替换成它们在 $\kappa(v)$ 的像 $\tilde{a}_i$, 则我们得到 E 在 v 处的约化

$$\tilde{E}/\kappa(v) : y^2 + \tilde{a}_1xy + \tilde{a}_3y = x^3 + \tilde{a}_2x^2 + \tilde{a}_4x + \tilde{a}_6.$$

如果 $\tilde{E}$ 仍然是光滑的, 我们称 E 在 v 处有**好约化**. 若不然, $\tilde{E}$ 的非奇异点有群结构, 且 $\tilde{E}(\bar{\kappa}(v))$ 同构于 $\bar{\kappa}(v)^\times$ 或 $\bar{\kappa}(v)$, 此时称 E 在 v 处有**乘法约化**或**加法约化**, 统称为**坏约化**. 若 $\kappa(v)$ 的特征整除 a_v 且 v 处是好约化, 则称在 v 处有**超奇异约化**. 如果 E 在 v 处有乘法约化, 根据 $\tilde{E}$ 在奇异点处的斜率是否落在 $\kappa(v)$ 中, 我们将其分为**分裂的乘法约化**和**不分裂的乘法约化**.

令

$$a_v = \#\kappa(v) + 1 - \#\tilde{E}(\kappa(v)),$$

则在坏约化时,

$$a_v = \begin{cases} 0, & v \text{ 为加法约化;} \\ 1, & v \text{ 为分裂的乘法约化;} \\ -1, & v \text{ 为不分裂的乘法约化.} \end{cases}$$

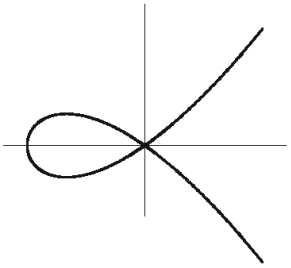

图 2.2　乘法约化

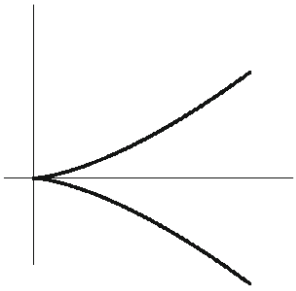

图 2.3　加法约化

定义 E 的 L 函数为

$$L(E/F,s)=\prod_{v\text{ 为坏约化}}(1-a_v\#\kappa(v)^{-s})^{-1}\cdot\prod_{v\text{ 为好约化}}(1-a_v\#\kappa(v)^{-s}+\#\kappa(v)^{1-2s})^{-1},$$

它在 Re$s>2$ 时收敛, 参见 [Kna, X§2 命题 10.4].

猜想 2.8.2. *L 函数 $L(E/F,s)$ 可以解析延拓至整个复平面, 而且满足关于 s 和 $2-s$ 的函数方程.*

L 函数是同源不变量.

2.9　导子

椭圆曲线 E/F 的**导子**是 F 上的一个反映约化情形的理想, 而且它是同源不变量. 对 F 的素位 v, 定义 E 的导子在 v 处的指数为

$$f_v=\begin{cases}0, & v\text{ 为好约化;}\\ 1, & v\text{ 为乘法约化;}\\ 2+\delta_v, & v\text{ 为加法约化,}\end{cases}$$

其中 δ_v 是惯性群在 Tate 模上的野分歧指数. E/F 的导子定义为

$$N_{E/F}=\prod_{\text{有限素位 }v}v^{f_v}.$$

2.10　Drinfeld 模

设 F 为函数域, 我们固定 F 的一个素位 ∞, $\mathcal{O}_F$ 为 F 中在 ∞ 以外的素位均正则的元素构成的环. 令 F_∞ 为 F 在 ∞ 的完备化, C 为 F_∞ 的代数闭包.

令 k 为特征 p 环且有单同态 $A \to k$. 令 $k\{\tau\}$ 为 τ 的非交换多项式环使得 $\tau a = a^p \tau$. 自然嵌入 $\epsilon : k \hookrightarrow k\{\tau\}$ 有左逆 $D : k\{\tau\} \to k, D(\sum a_n \tau^n) = a_0$. 如果 R 是 k 代数, 则加法群 R 可以视为 $k\{\tau\}$ 模:

$$(\sum a_n \tau^n)(x) = \sum a_n x^{p^n}.$$

k 上的 **Drinfeld 模**是环同态 $\phi : A \to k\{\tau\}$ 使得 $\phi(A) \not\subseteq k$ 且 $D \circ \phi$ 是给定的同态. ϕ 的**秩**为正整数 r 使得 $p^{\deg_\tau(\phi(a))} = \#(A/a)^r$. 非零映射 $u : \phi \to \phi'$ 称为**同源**, 如果 $u\phi(a) = \phi'(a)u$. 对于 $\mathcal{O}_F$ 的非零理想 N, 令 $Y_0(N)$ 为秩 2 带 "N 循环同源结构" 的 Drinfeld 模的模参数化空间, 其 "Drinfeld 紧化" $X_0(N)$ 是光滑本征刚性空间且

$$X_0(N)(C) = \mathrm{GL}_2(F)\backslash(\Omega(C) \cup \mathbb{P}^1(F)) \times \mathrm{GL}_2(\mathbb{A}_f)/U_0(N),$$

其中 $\Omega(C) = \mathbb{P}^1(C) - \mathbb{P}^1(F_\infty)$ 是 Drinfeld 上半平面, 参见 [Gek, SS3, V], [GeR, §8] 和 [WeY].

2.11　模性

2.11.1　$F = \mathbb{Q}$

当 $F = \mathbb{Q}$ 时, 设 N 是 E 的导子 (参见 [Sil, 附录 C§16]), 令 $Y_0(N)$ 为带 N 循环子群 ($\cong \mathbb{Z}/N\mathbb{Z}$) 结构的椭圆曲线的模参数化空间, $X_0(N)$ 为它的紧化后的模曲线. 根据 Wiles, Breuil, Conrad, Diamond 和 Taylor 的定理, 存在权为 2 水平为 N 的模形式 f 使得 $L(E, s) = L(f, s)$. 这等价于存在非常值态射

$$X_0(N) \to E.$$

由此, 我们得知 $L(E, s)$ 存在函数方程

$$\Lambda(E, s) = w(E)\Lambda(E, 2 - s), \tag{2.7}$$

其中 $\Lambda(E, s) = N^{s/2}(2\pi)^{-s}\Gamma(s)L(E, s)$, $w(E) = \pm 1$ 被称为 E 的**根数**, 参见 [Kna, 定理 9.8].

模映射 $X_0(N) \to E$ 的构造如下:

$$X_0(N) \to J_0(N) = \mathrm{Jac}(X_0(N)) \to J_0(N)/(T_n - a_n; n \nmid N) \xrightarrow{h} E.$$

这里 $\mathrm{Jac}(X_0(N))$ 是 $X_0(N)$ 的 Jacobian, T_n 是 Hecke 算子, a_n 是 $L(E, s)$ 的 Fourier 系数, N 是 E 的导子, h 是同源. 回忆 Atkin–Lehner 算子在数域情形在 $X_0(N)$ 上的作用为 $w_N(x) = \frac{1}{Nx}$. 由于 w_N 的作用于 T_n 交换, 因此 w_N 诱导了在 E 上的群同态 $-w(E)$.

2.11.2　F 为函数域

当 F 是函数域时, 我们固定 F 的无穷素位 ∞. 此时 Atkin–Lehner 算子在带 N 循环子群 Z 的 Drinfeld 模 D 的作用为

$$w_N = \prod_{\mathfrak{p}|N} w_{\mathfrak{p}},$$

$$w_{\mathfrak{p}}(D, Z) = (D/Z_{\mathfrak{p}^k}, (D_{\mathfrak{p}^k} + Z)/Z_{\mathfrak{p}^k}), \quad \mathfrak{p}^k \parallel N.$$

假设 E 在 ∞ 处有分裂的乘性约化, 导子为 $N_E = N\infty$. Deligne, Drinfeld 和 Zarhin 证明了此时 E 的模性, 因此存在非常值态射

$$X_0(N) \to E.$$

该映射的构造与 $F = \mathbb{Q}$ 情形类似. 此时 w_N 的阶为 $2d_N$, 其中 d_N 为 N 在理想类群 $\mathrm{Pic}(\mathcal{O}_F)$ 中的阶. 因此 $w = w_N^{d_N}$ 为对合且 w 诱导了 E 上的群同态 $-w(E)$.

2.12　BSD 猜想

Birch 和 Swinnerton-Dyer 猜想是指

$$r = \mathrm{rank}\, E(F) = \mathrm{ord}_{s=1} L(E/F, s),$$

而且 $L(E/F, s)$ 的 Taylor 展开的首项系数有如下表达式:

$$\frac{1}{r!} L^{(r)}(E/F, s) = \frac{Ш\ R\tau}{(\#E_{\mathrm{tor}}(F))^2},$$

其中 R 是单元基准, τ 是玉河数.

2.12.1　数域情形

当 F 为数域时, 我们已经知道 $\mathrm{ord}_{s=1} L(E/\mathbb{Q}, s) \leq 1$ 时, 弱 BSD 猜想成立. 当 $\mathrm{ord}_{s=1} L(E/\mathbb{Q}, s) = 0$ 时, 精确 BSD 猜想的 $p \geq 5$ 部分成立; 当 $\mathrm{ord}_{s=1} L(E/\mathbb{Q}, s) = 1$ 时, 精确 BSD 猜想的 $p \nmid 6N_{E/\mathbb{Q}}$ 部分成立.

2.12.2　函数域情形

函数域情形根据 Tate, Milne, Kato 和 Trihan 等人的结果我们知道

$$\mathrm{rank}\, E(F) \leq \mathrm{ord}_{s=1} L(E/F, s),$$

且等式成立当且仅当下述 Tate–Shafarevich 群的任一 l 部分有限. 而且等式成立时, 精确 BSD 猜想也成立.

如果函数域上椭圆曲线 E 的 Weierstrass 方程的系数 $a_i \in \mathbb{F}_q$, 则称其为**常椭圆曲线**. 如果 E 在 F 的有限扩张 K 上是常椭圆曲线, 称其为 **isotrivial 椭圆曲线**.

我们已经知道在一些情形下上述等式成立. 如果上述等式对于 E/K 成立, 若 K 是 F 的有限扩张, 则上述等式对于 E/F 成立. 上述等式对于常椭圆曲线成立, 从而对于 isotrivial 椭圆曲线也成立. 若 E 的 Nèron 模型是有理曲面, K_3 曲面或被曲线乘积所控制, 则上述等式也成立.

第三章　2 下降法与非同余数

本章基于我们发表的论文 [OuZ, OuZ2].

3.1　同余数

定义 3.1.1. *如果正整数 n 能表示为一个有理边长直角三角形的面积, 称 n 为*同余数*. 否则称之为*非同余数*.*

容易看出 n 是同余数等价于 nt^2 是同余数, 其中 t 是任意的正整数. 因此我们只考虑无平方因子的 n.

设有理边长的直角三角形三条边分别为 a, b, c, 则 $a^2 + b^2 = c^2$. 设 $t = (c + b)/a \in \mathbb{Q}$, 则 $c - b = at^{-1}$, 因此

$$b = a(t - t^{-1})/2, \quad c = a(t + t^{-1})/2.$$

于是 $n = a^2(t - t^{-1})/4$, $(nt, 2n^2ta^{-1})$ 是椭圆曲线

$$E_1 : y^2 = x^3 - n^2x \tag{3.1}$$

的一个有理点. 根据 Lutz–Nagell 定理 (参见 [Kna, V§1 定理 5.1]), E_1 的有限阶 $\mathbb{Q}$ 点为

$$E_{1,\mathrm{tor}}(\mathbb{Q}) = \{(0, 0), (\pm n, 0), O\}. \tag{3.2}$$

如果 (x, y) 是 E_1 的一个无限阶点, 则 $x \neq \pm n, y \neq 0$,

$$\frac{x^2 + n^2}{y}, \frac{x^2 - n^2}{y}, \frac{2xn}{y}$$

的绝对值构成一个面积为 n 的直角三角形. 因此:

命题 3.1.2. *(1) n 是同余数当且仅当 $E_1(\mathbb{Q})$ 的秩大于等于 1.*
(2) n 是非同余数当且仅当 $E_1(\mathbb{Q})$ 的秩等于 0.

命题 3.1.3. *$n \equiv 5, 6, 7 \bmod 8$ 时 E_1 的根数为 -1, 因此 $L(E_1, s)$ 在 $s = 1$ 处的阶为奇数.*

证明. 参见 [Kob, II §5 定理]. □

由此可知, 如果 BSD 猜想成立, 则 $n \equiv 5, 6, 7 \bmod 8$ 是同余数. 在同余数方面, 我们有如下结果:

命题 3.1.4 (Heegner)**.** *$p \equiv 5, 7$ 或 $2p \equiv 6 \bmod 8$ 是同余数, 其中 p 是素数.*

证明. 参见 [Hee]. □

命题 3.1.5 (田野)**.** *对任意正整数 k, 存在无穷多个同余数恰好有 k 个素因子.*

证明. 参见 [Tia]. □

在非同余数方面, 我们有如下结果:

命题 3.1.6 (Fermat)**.** *1 和 2 是非同余数.*

我们将利用 2 下降法给出 2 是非同余数的证明. 该方法本质上是将椭圆曲线上的点 P 下降为 $\pm\frac{1}{2}P$. Mordell 证明 $E(F)$ 是有限生成阿贝尔群时, 也是先证明了 $E(F)/2E(F)$ 有限, 然后利用 2 下降法得以证明.

命题 3.1.7 (Fermat)**.** *$u^4+v^4=w^2$ 没有正整数解.*

证明. 假设有正整数解. 我们不妨设 u,v 互素且 u 是奇数, v 是偶数, 则

$$(w+u^2)(w-u^2)=v^4.$$

因此 $w+v^2$ 和 $w-v^2$ 均是平方数. 设 $w+v^2=m^2, w-v^2=n^2, m>n>0$. 由于 m,n 均是奇数, 设 $m'=(m+n)/2, n'=(m-n)/2$, 则

$$w=m'^2+n'^2,\ v^2=2m'n',\ u^2=m'^2-n'^2,$$

且 m',n' 互素. 由于 $m'^2=u^2+n'^2$, 类似地, 我们有

$$m'=p^2+q^2,\ u=p^2-q^2,\ n'=2pq,$$

p,q 互素. 于是

$$\left(\frac{v}{2}\right)^2=pq(p^2+q^2).$$

由于 p,q,p^2+q^2 两两互素, 因此

$$p=r^2,\ q=s^2, p^2+q^2=t^2,$$

$r^4+s^4=t^2$. 容易知道 $rs\neq 0$ 且 $\max\{|r|,|s|\}<\max\{|u|,|v|\}$. 于是我们找到了一组 "更小" 的解, 这不可能无限操作下去, 因此原方程没有正整数解. □

如果 2 是同余数, 则 $y^2=x^3-4x$ 有非平凡解 (x,y), 于是

$$(y^2+8x)^2=y^4+(2x)^4,$$

因此 $u^4+v^4=w^2$ 有正整数解, 这不可能! 因此 2 是非同余数.

如果我们沿用第 2.7 节的记号, 则由引理 2.7.1 可知 $\mathrm{Sel}^{(\phi)}(E_1/\mathbb{Q})$ 的大小为 4. 由基本正合列(2.6)可知 $\mathrm{rank}\, E(\mathbb{Q})=0$, 从而 2 是非同余数. 由此可见, 利用现代记号可以将 2 下降法的过程大大简化.

利用 2 下降法, 我们有:

命题 3.1.8 (冯克勤)**.** *对任意正整数 k, 存在无穷多个 Tate–Shafarevich 群 2 部分平凡的非同余数恰好有 k 个素因子.*

证明. 参见 [冯]. □

根据 Monsky 的结果 [HeB], 我们可以完全确定所有 Tate–Shafarevich 群 2 部分平凡的非同余数. 李德琅和田野 [LiT] 利用二阶 2 下降法对 Selmer 群进行了进一步的估计并找到了一系列 Tate–Shafarevich 群 2 部分非平凡的非同余数. 在本章中, 我们将利用该方法找到更多的 Tate–Shafarevich 群 2 部分非平凡的非同余数.

3.2　记号和结论

对于无平方因子的正整数 n, E_i 和 E_i' $(i=1,2,3)$ 是如下的椭圆曲线

$$E_1: y^2 = x^3 - n^2x, \quad E_1': y^2 = x^3 + 4n^2x,$$

$$E_2: y^2 = x(x+n)(x+2n), \quad E_2': y^2 = x^3 - 6nx^2 + n^2x,$$

$$E_3: y^2 = x(x-n)(x-2n), \quad E_3': y^2 = x^3 + 6nx^2 + n^2x.$$

E_i 被称为**同余椭圆曲线**, E_i' 为其对偶. E_i 之间两两同构. 由于这些曲线相互同源, 因此它们具有相同的秩. 由引理 3.1.2知, n 是非同余数当且仅当其中任意一条 (或全部) 的秩为零.

设 p 是素数. $v = v_p$ 表示规范的 p 进赋值, 即 $v(p) = 1$. 记号 $O(y)$ 表示 p 进赋值 $\geq v(y)$ 的数. 对于赋值为偶数的有理数或 p 进数 x, 我们将 Legendre 符号修改为

$$\left(\frac{x}{p}\right) := \left(\frac{xp^{-v_p(x)}}{p}\right). \tag{3.3}$$

对于整数 $m \geq 2$, 我们将 Jacobi 符号 $\left(\frac{\cdot}{m}\right)$ 修改为

$$\left(\frac{x}{m}\right) = \prod_{p|m} \left(\frac{x}{p}\right)^{v_p(m)}. \tag{3.4}$$

令

$$\left[\frac{x}{m}\right] := (1 - \left(\frac{x}{m}\right))/2 \tag{3.5}$$

为**加性 Jacobi 符号** (或**加性 Legendre 符号**, 如果 m 是素数的话). $\left(\frac{\cdot}{m}\right)$ 或 $\left[\frac{\cdot}{m}\right]$ 诱导了 $\{x \in \mathbb{Q}^\times/\mathbb{Q}^{\times 2} : \text{对任意 } p \mid m, v_p(x) \text{ 是偶数 }\}$ 到 $\{\pm 1\}$ 或 2 元域 $\mathbb{F}_2$ 的同态.

(a,b) 表示非零整数 a 和 b 的最大公因子. 令 m 为 n 的奇数部分, 即 $n = (2,n)m$. 设 $m = p_1 \cdots p_k$ 是 m 的素因子分解.

本文中所有矩阵和向量都定义在 $\mathbb{F}_2$ 上. 令 A 为 $k\times k$ 矩阵, 其中 (i,j) 元为 $\left[\frac{p_j}{p_i}\right]$, 如果 $i\neq j$; 为 $\left[\frac{m/p_i}{p_i}\right]$, 如果 $i=j$. 令

$$C_a=\mathrm{diag}\{\left[\frac{a}{p_1}\right],\cdots,\left[\frac{a}{p_k}\right]\},$$

$$\overrightarrow{0}=(0,\cdots,0)^{\mathrm{T}},\ \overrightarrow{1}=(1,\cdots,1)^{\mathrm{T}}.$$

对于向量 $\overrightarrow{v}=(v_1,\cdots,v_k)^T\in\mathbb{F}_2^k$, 令

$$d(\overrightarrow{v}):=\prod_{i:\ v_i=1}p_i.$$

特别地, $d(\overrightarrow{0})=1, d(\overrightarrow{1})=m$. 反过来, 对于 $2m$ 的因子 d, 令 $\overrightarrow{v}(d):=(v_1,\cdots,v_k)^T$ 使得

$$v_i=\begin{cases}1, & \text{若 } p_i\mid d;\\ 0, & \text{若 } p_i\nmid d.\end{cases}$$

注意 $d(\overrightarrow{v}(d))=d/(d,2)$ 不一定等于 d.

定理 3.2.1. (1) 设 $n\equiv 1 \bmod 8$, $p_i\equiv 1 \bmod 4$, $\mathrm{rank}\,A=k-1$. 设 $\overrightarrow{v}$ 是方程 $A\overrightarrow{x}=C_2\overrightarrow{1}$ 的一个根, 令 $d=d(\overrightarrow{v})$. 令 $2d=\tau^2+\mu^2$, 选取 $\sqrt{-1}\in\mathbb{Z}/n\mathbb{Z}$ 使得对任意 $p\mid d$, $p\mid\tau-\sqrt{-1}\mu$. 若 $\left(\frac{\tau+\sqrt{-1}\mu}{n}\right)\left(\frac{2}{d}\right)=-1$, 则 n 是非同余数.

特别地, 如果 $p_i\equiv 1 \bmod 8$, $\mathrm{rank}\,A=k-1$, $\left(\frac{1+\sqrt{-1}}{n}\right)=-1$, 则 n 是非同余数.

(2) 设 $m\equiv 1 \bmod 8$, $p_i\equiv\pm 1 \bmod 8$, $\mathrm{rank}\,A=\mathrm{rank}(A+C_{-1})=k-1$. 令 $m=2\mu^2-\tau^2$. 若 $|\mu|\equiv 3 \bmod 4$, 则 $n=m$ 是非同余数. 若 $\left(\frac{2+\sqrt{2}}{m}\right)=-1$, 则 $n=2m$ 是非同余数.

注 3.2.2. (1) 由于 $A\overrightarrow{1}=0$, 因此 A 是奇异阵. (1) 中 $\mathrm{rank}\,A=k-1$ 意味着 A 的像空间为 $x_1+\cdots+x_k=0$, 这包含 $C_2\overrightarrow{1}$. 因此方程 $A\overrightarrow{x}=C_2\overrightarrow{1}$ 有解, 且 $\overrightarrow{v}$ 和 $\overrightarrow{v}+\overrightarrow{1}$ 是它的全部解. 如果我们将 $\overrightarrow{v}$ 替换为 $\overrightarrow{v}'=\overrightarrow{v}+\overrightarrow{1}$, 并相应地把 d,τ,μ,i 替换位 $d'=n/d$, τ',μ',i', 则 $\left[\frac{2}{d}\right]=\left[\frac{2}{n/d}\right]$,

$$\left[\frac{\tau+\mu i}{n}\right]=\left[\frac{\tau+\mu i}{d}\right]+\left[\frac{\tau+\mu i'}{n/d}\right].$$

令 $u=(\tau\tau'-\mu\mu')/2$, $v=(\tau\mu'-\mu\tau')/2$, 则

$$\begin{aligned}u+vi=&(\tau+\mu i)(\tau'+\mu' i)/2\equiv\tau(\tau'+\mu'\cdot\frac{\tau}{\mu})\\ \equiv&\tau\mu(\tau'\mu+\tau\mu')/\mu^2\equiv(\tau+\mu)^2/\mu^2\cdot v/2 \bmod d.\end{aligned}$$

类似地, $u+vi' \equiv (\tau'+\mu')^2/\mu'^2 \cdot v/2 \bmod (n/d)$. 如果我们将 d 和 n/d 对换, $\left[\frac{\tau+\sqrt{-1}\mu}{n}\right]+\left[\frac{2}{d}\right]$ 将会相差

$$\begin{aligned}&\left[\frac{\tau+\mu i}{d}\right]+\left[\frac{\tau+\mu i'}{n/d}\right]+\left[\frac{\tau'+\mu' i'}{n/d}\right]+\left[\frac{\tau'+\mu' i}{d}\right]\\ =&\left[\frac{2(u+vi)}{d}\right]+\left[\frac{2(u+vi')}{n/d}\right]=\left[\frac{v}{d}\right]+\left[\frac{v}{n/d}\right]\\ =&\left[\frac{v}{n}\right]=\left[\frac{n}{v}\right]=\left[\frac{u^2+v^2}{v}\right]=0\in\mathbb{F}_2.\end{aligned}$$

因此 (1) 中的条件不依赖于选取 d 还是 n/d.

(2) 容易验证 (2) 中 (τ,μ) 可能的值为 (τ_k,μ_k), 其中

$$\tau_k+\sqrt{2}\mu_k=(\tau_0+\sqrt{2}\mu_0)(3+2\sqrt{2})^k.$$

由此经计算可得 $\mu_k\equiv\mu_0 \bmod 4$ 且 μ_k 和 μ_0 符号相同.

(3) *Monskey* 证明了 $\mathrm{Sel}^{(2)}(E_i/\mathbb{Q})/E_{i,\mathrm{tor}}(\mathbb{Q})$ 的 $\mathbb{F}_2$ 维数为

$$2k-\operatorname{rank}\begin{pmatrix}A+C_{-2} & C_2\\ C_2 & A+C_2\end{pmatrix}.$$

因此我们很容易确定所有的 *Tate–Shafarevich* 群的 2 部分平凡的秩零同余椭圆曲线, 所以我们只关心 *Tate–Shafarevich* 群的 2 部分平凡的秩零同余椭圆曲线, 参见 [HeB].

例 3.2.3. 在 (1) 中, 令 $n=5\times13\times41$, 则 $A=\begin{pmatrix}1&1&0\\1&0&1\\0&1&1\end{pmatrix}$ 的秩为 2, $\overrightarrow{d}=(1,0,0)^{\mathrm{T}}$, $d=5, n/d=533$, $2d=3^2+1^2, 2n/d=29^2+15^2$,

$$\left[\frac{3+\sqrt{-1}}{5}\right]=0,\ \left[\frac{3+\sqrt{-1}}{13}\right]=1,\ \left[\frac{3+\sqrt{-1}}{41}\right]=1,$$

$$\left[\frac{29+15\sqrt{-1}}{5}\right]=0,\ \left[\frac{29+15\sqrt{-1}}{13}\right]=1,\ \left[\frac{29+15\sqrt{-1}}{41}\right]=1,$$

因此 $\left[\frac{3+\sqrt{-1}}{n}\right]+\left[\frac{2}{5}\right]=\left[\frac{29+15\sqrt{-1}}{n}\right]+\left[\frac{2}{533}\right]=1$, 从而 $5\times13\times41$ 是非同余数.

在 (2) 中, 令 $n=7\times23\times41$, 则 $A=\left(\begin{smallmatrix}1&0&1\\1&1&0\\1&0&1\end{smallmatrix}\right)$ 和 $A+C_{-1}=\left(\begin{smallmatrix}0&0&1\\1&0&0\\1&0&1\end{smallmatrix}\right)$ 的秩为 2, $n=6601=2\times59^2-19^2$, 因此 $7\times23\times41$ 是非同余数. 令 $n=2\times23\times31$, 则 $A=\left(\begin{smallmatrix}0&0\\1&1\end{smallmatrix}\right)$ 和 $A+C_{-1}=\left(\begin{smallmatrix}1&0\\1&0\end{smallmatrix}\right)$ 的秩为 1, $\left(\frac{2+\sqrt{2}}{m}\right)=\left(\frac{7}{23}\right)\left(\frac{10}{31}\right)=-1$, 因此 $2\times23\times31$ 是非同余数.

3.3　2 下降法

本节我们将回顾如何利用 2 下降法计算椭圆曲线的 Selmer 群, 参见 [LiT, 232–233 页], [BSD, §5] 和 [Sil, X 4]. 对于 K 上椭圆曲线的同源 $\varphi : E \to E'$, 我们有基本正合列 (参见 §2.6)

$$0 \to E'(K)/\varphi E(K) \to \mathrm{Sel}^{(\varphi)}(E/K) \to Ш\,(E/K)[\varphi] \to 0. \tag{3.6}$$

如果 $\psi : E' \to E$ 也是同源, 则对于复合映射 $\psi \circ \varphi : E \to E$, 我们有如下交换图 (参见 [XiZ, 5 页]):

$$\begin{array}{ccccccccc}
 & & & & & & 0 & & \\
 & & & & & & \downarrow & & \\
0 & \longrightarrow & E'(K)/\varphi E(K) & \longrightarrow & \mathrm{Sel}^{(\varphi)}(E/K) & \longrightarrow & Ш\,(E/K)[\varphi] & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \psi} & & \downarrow{\scriptstyle \psi_S} & & \downarrow & & \\
0 & \longrightarrow & E(K)/\psi\varphi E(K) & \longrightarrow & \mathrm{Sel}^{(\psi\varphi)}(E/K) & \longrightarrow & Ш\,(E/K)[\psi\varphi] & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow{\scriptstyle \mathrm{res}} & & \downarrow & & \\
0 & \longrightarrow & E(K)/\psi E'(K) & \longrightarrow & \mathrm{Sel}^{(\psi)}(E'/K) & \longrightarrow & Ш\,(E'/K)[\psi] & \longrightarrow & 0 \\
 & & \downarrow & & & & & & \\
 & & 0 & & & & & &
\end{array} \tag{3.7}$$

我们记限制映射 res 的像为 $\widetilde{\mathrm{Sel}}^{(\psi)}(E'/K)$. 如果 φ 次数为 n, ψ 是其对偶, 则由上述图表可以看出, 对 Sel 和 $\widetilde{\mathrm{Sel}}$ 的估计可以得到弱 Mordell–Weil 群和 Tate–Shafarevich 群.

从现在起, 我们取 $K = \mathbb{Q}$. 对于 $a, b \in \mathbb{Q}$, 令

$$\begin{aligned}
E = E_{a,b} :&\quad y^2 = x^3 + ax^2 + bx, \\
E' = E_{-2a,a^2-4b} :&\quad y^2 = x^3 - 2ax^2 + (a^2 - 4b)x,
\end{aligned}$$

则

$$\varphi = \varphi_{a,b} : E \to E', \quad (x, y) \mapsto \left(\frac{y^2}{x^2}, \frac{y(b - x^2)}{x^2} \right)$$

是次数为 2 的同源. 它的对偶为 $\psi = \lambda \circ \varphi_{-2a,a^2-4b}$, 其中 $\lambda : E_{4a,16b} \to E_{a,b}, (x, y) \mapsto (x/4, y/8)$ 是同构.

注 3.3.1. *我们将要计算 Selmer 群* $\mathrm{Sel}^{(\varphi)}(E/\mathbb{Q})$, $\widetilde{\mathrm{Sel}}^{(\varphi)}(E/\mathbb{Q})$ *(对上述图表取* $\varphi \circ \psi$*)* *和* $\mathrm{Sel}^{(\psi)}(E'/\mathbb{Q})$, $\widetilde{\mathrm{Sel}}^{(\psi)}(E'/\mathbb{Q})$ *(对上述图表取* $\psi \circ \varphi$*).* *由于* $\psi = \lambda \circ \varphi_{-2a,a^2-4b}$, *对* ψ *的 Selmer 群的计算与* φ *类似, 只需将* (a, b) *替换为* $(-2a, a^2 - 4b)$.

记

$$S = \{\infty, p \mid 2b(a^2-4b)\},$$

$$\mathbb{Q}(S,2) := \{b \in \mathbb{Q}^\times/\mathbb{Q}^{\times 2} : \text{对任意} p \notin S, v_p(b) \text{是偶数}\}.$$

$2b(a^2-4b)$ 所有无平方因子的约数可以代表整个集合 $\mathbb{Q}(S,2)$, 我们将不加区分地使用它们.

引理 3.3.2 ([Sil], X.4)**.** *令 C_d 和 C'_d 是 $d \in \mathbb{Q}(S,2)$ 对应的 E 和 E' 的齐性空间*

$$C_d:\ dw^2 = d^2 - 2adz^2 + (a^2-4b)z^4, \qquad C'_d:\ dw^2 = d^2 + adz^2 + bz^4.$$

则 Selmer 群 $\mathrm{Sel}^{(\varphi)}(E/\mathbb{Q})$ *和* $\mathrm{Sel}^{(\psi)}(E'/\mathbb{Q})$ *可以等同于*

$$\mathrm{Sel}^{(\varphi)}(E/\mathbb{Q}) = \{d \in \mathbb{Q}(S,2) : \text{对任意} v \in S, C_d(\mathbb{Q}_v) \text{非空}\},$$

$$\mathrm{Sel}^{(\psi)}(E'/\mathbb{Q}) = \{d \in \mathbb{Q}(S,2) : \text{对任意} v \in S, C'_d(\mathbb{Q}_v) \text{非空}\}.$$

设 $d \in \mathrm{Sel}^{(\varphi)}(E/\mathbb{Q})$. 由 Hasse-Minkowski 定理 (参见 [Ser]) 知方程 $d\sigma^2 = d^2\tau^2 - 2ad\tau\mu + (a^2-4b)\mu^2$ 存在一个非零整数解 (σ,τ,μ). 对于 $s \in \mathbb{Q}^\times/\mathbb{Q}^{\times 2}$, 定义曲线 $\mathcal{M}_s$ 为

$$\mathcal{M}_s : \begin{cases} dw^2 = d^2t^4 - 2adt^2z^2 + (a^2-4b)z^4, \\ d\sigma w - (d\tau - a\mu)(dt^2 - az^2) - 4b\mu z^2 = su^2. \end{cases} \tag{3.8}$$

则类似于 [BSD, §5 引理 8 和 10] , 我们可以得到关于 $\widetilde{\mathrm{Sel}}$ 的如下引理:

引理 3.3.3. *$d \in \widetilde{\mathrm{Sel}}^{(\varphi)}(E/\mathbb{Q})$ 当且仅当存在 $s \in \mathbb{Q}(S,2)$ 使得 $\mathcal{M}_s$ 局部处处有解.*

证明. 令 $w = (x_1 - b/x_1)/\sqrt{d}$, $t = y_1/(\sqrt{d}x_1)$, $z = 1$, 其中 $(x_1,y_1) \in E$, 则 $d \in \mathrm{Sel}^{(\varphi)}(E/\mathbb{Q})$ 对应的齐性空间为

$$C_d : dw^2 = d^2t^4 - 2adt^2z^2 + (a^2-4b)z^4.$$

我们有交换图表

$$\begin{array}{ccccc} E' & \xrightarrow{\psi} & E & \xrightarrow{\varphi} & E' \\ & & \updownarrow & \nearrow & \\ & & C_d & & \end{array} \tag{3.9}$$

若 $d \in \widetilde{\mathrm{Sel}}^{(\varphi)}(E/\mathbb{Q})$, $\psi(x_2,y_2) = (x_1,y_1)$, 则 $x_1 = y_2^2/(4x_2^2)$. 取

$$u = \sqrt{\frac{\sqrt{d}\sigma - (d\tau - a\mu)}{s}} \cdot \frac{x_2(2x_1\mu + \sqrt{d}\sigma + d\tau - a\mu)}{\mu y_2},$$

则经过一些计算之后, 我们可以得到方程 (3.8). 证明的其余部分与 [BSD, §5 引理 8 和 10] 相同. □

3.4　同余椭圆曲线情形

我们将上述结论应用到同余椭圆曲线情形. 令 $(a,b)=(0,-n^2),(3n,2n^2)$ 或 $(-3n,2n^2)$, 则相应地 $(-2a,a^2-4b)=(0,4n^2)$, $(-6n,n^2)$ 或 $(6n,n^2)$, 我们得到了 §3.2 中的椭圆曲线 E_i 和 E_i'. 在这种情形, $S=\{\infty, 2m \text{ 的素因子}\}$, $\mathbb{Q}(S,2)$ 一一对应于 $2m$ 的所有因子.

取图表(3.7)中的同源为 $\psi\circ\varphi: E_i\to E_i$ 和 $\varphi\circ\psi: E_i'\to E_i'$. 第一种情形中 ψ 和 ψ_S 都是单射, 第二种情形中

$$\ker\Big(\varphi:\ \frac{E(\mathbb{Q})}{\psi E'(\mathbb{Q})}\to\frac{E'(\mathbb{Q})}{2E'(\mathbb{Q})}\Big)=\ker\Big(\varphi_S:\ \text{Sel}^{(\psi)}(E'/\mathbb{Q})\to\text{Sel}^{(2)}(E'/\mathbb{Q})\Big)$$

等于 $\mathbb{Z}/2\mathbb{Z}$. 下述命题告诉我们, 如果 $\tilde{S}$ 达到极小, 则 n 是非同余数.

命题 3.4.1. 令 $E=E_i$, $E'=E_i'$.

(1) 若 $\widetilde{\text{Sel}}^{(\varphi)}(E/\mathbb{Q})$ 的大小为 1, $\widetilde{\text{Sel}}^{(\psi)}(E'/\mathbb{Q})$ 的大小为 4, 则

$$\text{rank}\,E(\mathbb{Q})=\text{rank}\,E'(\mathbb{Q})=0. \tag{3.10}$$

而且若 $\text{Sel}^{(\varphi)}(E/\mathbb{Q})$ 大小为 1, 则

$$Ш\,(E/\mathbb{Q})[2^\infty]=0,\quad Ш\,(E'/\mathbb{Q})[2^\infty]\cong\text{Sel}^{(\psi)}(E'/\mathbb{Q})/(\mathbb{Z}/2\mathbb{Z})^2; \tag{3.11}$$

若 $\text{Sel}^{(\psi)}(E'/\mathbb{Q})$ 大小为 4, 则

$$Ш\,(E/\mathbb{Q})[2^\infty]\cong\text{Sel}^{(\varphi)}(E/\mathbb{Q}),\quad Ш\,(E'/\mathbb{Q})[2^\infty]=0. \tag{3.12}$$

(2) 若 $\#\widetilde{\text{Sel}}^{(\varphi)}(E/\mathbb{Q})<4$ 且 $\text{rank}_{\mathbb{F}_2}\text{Sel}^{(\varphi)}(E/\mathbb{Q})$ 是偶数, 则 $\#\widetilde{\text{Sel}}^{(\varphi)}(E/\mathbb{Q})=1$; 若 $\#\widetilde{\text{Sel}}^{(\psi)}(E'/\mathbb{Q})<16$ 且 $\text{rank}_{\mathbb{F}_2}\text{Sel}^{(\psi)}(E'/\mathbb{Q})$ 是偶数, 则 $\#\widetilde{\text{Sel}}^{(\psi)}(E'/\mathbb{Q})=4$.

证明. (1) 由于 $E(\mathbb{Q})_{\text{tor}}\cap\psi E'(\mathbb{Q})=\{O\}$ 且 $\#E(\mathbb{Q})_{\text{tor}}=4$, 由图表(3.7)知

$$4\le\#E(\mathbb{Q})/\psi E'(\mathbb{Q})\le\#\widetilde{\text{Sel}}^{(\psi)}(E'/\mathbb{Q}),$$

$$1\le\#E'(\mathbb{Q})/\varphi E(\mathbb{Q})\le\#\widetilde{\text{Sel}}^{(\varphi)}(E/\mathbb{Q}).$$

若 $\#\widetilde{\text{Sel}}^{(\varphi)}(E/\mathbb{Q})=1$, $\#\widetilde{\text{Sel}}^{(\psi)}(E'/\mathbb{Q})=4$, 则这些不等式都变成了等式, 于是 $\#E(\mathbb{Q})/2E(\mathbb{Q})=4$ 且 $\text{rank}\,E(\mathbb{Q})=\text{rank}\,E'(\mathbb{Q})=0$.

更进一步, 若 $\#\text{Sel}^{(\varphi)}(E/\mathbb{Q})=1$, 则

$$\text{Sel}^{(2)}(E/\mathbb{Q})=(\mathbb{Z}/2\mathbb{Z})^2,\qquad Ш\,(E/\mathbb{Q})[2]=0,$$

$$\text{Sel}^{(2)}(E'/\mathbb{Q})=\frac{\text{Sel}^{(\psi)}(E'/\mathbb{Q})}{\mathbb{Z}/2\mathbb{Z}},\qquad Ш\,(E'/\mathbb{Q})[2]=\frac{\text{Sel}^{(\psi)}(E'/\mathbb{Q})}{(\mathbb{Z}/2\mathbb{Z})^2}.$$

因此 $Ш\,(E/\mathbb{Q})[2^\infty]=0$ 且 $Ш\,(E/\mathbb{Q})[2^k\varphi]=0$. 由正合列

$$0\to Ш\,(E'/\mathbb{Q})[\psi]\to Ш\,(E'/\mathbb{Q})[2^k]\to Ш\,(E/\mathbb{Q})[2^{k-1}\varphi],$$

对于任意 $k \in \mathbb{N}_+$, 我们有 Ш $(E'/\mathbb{Q})[2^k] \cong$ Ш $(E'/\mathbb{Q})[\psi]$, 由此

$$Ш\,(E'/\mathbb{Q})[2^\infty] \cong Ш\,(E'/\mathbb{Q})[\psi] \cong \mathrm{Sel}^{(\psi)}(E'/\mathbb{Q})/(\mathbb{Z}/2\mathbb{Z})^2.$$

对 $\#\mathrm{Sel}^{(\psi)}(E'/\mathbb{Q}) = 4$ 情形同理.

(2) 由于 Tate–Shafarevich 群上面存在 Cassels 反对称双线性型 (参见 [BSD, 95 页] 或 [Cas]), $\mathrm{Sel}^{(\varphi)}(E/\mathbb{Q})$ 和 $\widetilde{\mathrm{Sel}}^{(\varphi)}(E/\mathbb{Q})$ 的 $\mathbb{F}_2$ 秩具有相同的奇偶性, 因此 $\widetilde{\mathrm{Sel}}^{(\varphi)}(E/\mathbb{Q}) = \{1\}$. 对 $\mathrm{Sel}^{(\psi)}(E'/\mathbb{Q})$ 情形同理. □

注 3.4.2. 由于 Ш $(E/\mathbb{Q})[2^\infty] = 0$ 时 $\mathrm{Sel}^{(2)}$ 达到极小, 这种情形很容易由 *Monsky* 的工作得到, 因此我们将不考虑这种情形.

3.5 Selmer 群 $\mathrm{Sel}^{(\varphi)}$ 和 $\mathrm{Sel}^{(\psi)}$

对于 $2m$ 的任一因子 d, 令 $d' = d/(2,d)$ 为 d 的奇数部分. 下述命题列出了 $C_{i,d}, C'_{i,d}$ 局部有解的条件, 由于只需要考虑赋值并利用 Hensel 引理, 我们将省略证明 (参见 [OuZ, XiZ]).

命题 3.5.1. (1) $C_{1,d}, C_{2,d}$ 和 $C'_{3,d}$ 在 $\mathbb{Q}_\infty$ 上有解当且仅当 $d > 0$; $C'_{1,d}, C'_{2,d}$ 和 $C_{3,d}$ 在 $\mathbb{Q}_\infty$ 上无解.

(2) C_d 在 $\mathbb{Q}_2$ 上有解的条件如下:

	n	d 是奇数	d 是偶数
$C_{1,d}$	奇数	$d \equiv 1 \bmod 4$	$d' \equiv 1 \bmod 4, n \equiv \pm 1 \bmod 8$
	偶数	$d \equiv 1 \bmod 8$	无解
$C_{2,d}$	奇数	$n \equiv 1 \bmod 4, d \equiv 1 \bmod 8$ 或 $n \equiv 3 \bmod 4, d \equiv \pm 1 \bmod 8$	无解
	偶数	$d \equiv 1 \bmod 8$	$m \equiv 7, d' \equiv 1 \bmod 8$ 或 $m \equiv 5, d' \equiv 7 \bmod 8$
$C_{3,d}$	奇数	$n \equiv 3 \bmod 4, d \equiv 1 \bmod 8$ 或 $n \equiv 1 \bmod 4, d \equiv \pm 1 \bmod 8$	无解
	偶数	$d \equiv 1 \bmod 8$	$m \equiv 1 \bmod 4, d' \equiv 1 \bmod 8$

C'_d 在 $\mathbb{Q}_2$ 上有解的条件如下:

	n	d 是奇数	d 是偶数
$C'_{1,d}$	奇数	d 或 $n/d \equiv \pm 1 \bmod 8$	无解
	偶数	有解	有解
$C'_{2,d}$	奇数	d' 或 $-n/d' \equiv 1 \bmod 4$	
	偶数	$m \equiv 1, 3$ 或 $m \equiv 5, d' \equiv 1, 3$ 或 $m \equiv 7, d' \equiv \pm 1 \bmod 8$	
$C'_{3,d}$	奇数	d' 或 $n/d' \equiv 1 \bmod 4$	
	偶数	$m \equiv 5, 7$ 或 $m \equiv 3, d' \equiv 1, 3$ 或 $m \equiv 1, d' \equiv \pm 1 \bmod 8$	

(3) 对于奇数 $p \mid n$, C_d 和 C'_d 在 $\mathbb{Q}_p$ 上有解的条件如下:

	$p \mid d$	$p \mid (2n/d)$
$C_{1,d}$	$p \equiv 1 \bmod 4, \left(\frac{n/d}{p}\right) = 1$	$\left(\frac{d}{p}\right) = 1$
$C_{2,d}$	$p \equiv \pm 1 \bmod 8, \left(\frac{n/d}{p}\right) = 1$	
$C_{3,d}$	$p \equiv \pm 1 \bmod 8, \left(\frac{-n/d}{p}\right) = 1$	
$C'_{1,d}$	$\left(\frac{n/d}{p}\right) = 1$ 对任意 $p \equiv 1 \bmod 4$	$\left(\frac{d}{p}\right) = 1$ 对任意 $p \equiv 1 \bmod 4$
$C'_{2,d}$	$\left(\frac{-n/d}{p}\right) = 1$ 对任意 $p \equiv \pm 1 \bmod 8$	$\left(\frac{d}{p}\right) = 1$ 对任意 $p \equiv \pm 1 \bmod 8$
$C'_{3,d}$	$\left(\frac{n/d}{p}\right) = 1$ 对任意 $p \equiv \pm 1 \bmod 8$	$\left(\frac{d}{p}\right) = 1$ 对任意 $p \equiv \pm 1 \bmod 8$

推论 3.5.2. (1) 假设 $n \equiv 1 \bmod 8$, $p_i \equiv 1 \bmod 4$, $\operatorname{rank} A = k-1$. 令 $\overrightarrow{v}$ 是方程 $A\overrightarrow{x} = C_2\overrightarrow{1}$ 的一个根, $d = d(\overrightarrow{v})$, 则

$$\text{Sel}^{(\varphi)}(E_1/\mathbb{Q}) = \{1, n, 2d, 2n/d\}, \quad \text{Sel}^{(\psi)}(E'_1/\mathbb{Q}) = \{\pm 1, \pm n\}.$$

(2) 假设 $m \equiv 1 \bmod 8$, $p_i \equiv \pm 1 \bmod 8$, $\operatorname{rank} A = \operatorname{rank}(A + C_{-1}) = k-1$. 令 $\overrightarrow{v}$ 是方程 $(A + C_{-1})\overrightarrow{x} = \overrightarrow{0}$ 的一个非零根, $d = d(\overrightarrow{v})$.

(i) 若 $n = m$, 则

$$\text{Sel}^{(\varphi)}(E_3/\mathbb{Q}) = \{1, d, -n, -n/d\}, \quad \text{Sel}^{(\psi)}(E'_3/\mathbb{Q}) = \{1, 2, n, 2n\}.$$

(ii) 若 $n = 2m$, 则

$$\text{Sel}^{(\varphi)}(E_3/\mathbb{Q}) = \begin{cases} \{1, 2, d, 2d\}, & \text{若 } d \equiv 1 \bmod 8; \\ \{1, 2, -m/d, -n/d\}, & \text{若 } d \equiv -1 \bmod 8, \end{cases}$$

且 $\text{Sel}^{(\psi)}(E'_3/\mathbb{Q}) = \{1, 2, m, n\}$.

证明. 我们只证明 (1), 其余类似.

设 $d \in \text{Sel}^{(\varphi)}(E_1/\mathbb{Q})$. 由命题 3.5.1(1) 和 (2) 知 $0 < d \mid 2n$. 若 d 是奇数, 则由命题 3.5.1(3) 知 $A\overrightarrow{v}(d) = \overrightarrow{0}$, 于是 $\overrightarrow{v} = \overrightarrow{0}$ 或 $\overrightarrow{1}$, $d = 1$ 或 n. 若 $d = 2d'$ 是偶数, 则由命题 3.5.1(3) 知 $A\overrightarrow{v}(d') = C_2\overrightarrow{1}$, 于是 $d = 2d(\overrightarrow{v})$ 或 $2n/d(\overrightarrow{v})$, 其中 $\overrightarrow{v}$ 是方程 $A\overrightarrow{x} = C_2\overrightarrow{1}$ 的一个解.

设 $d \in \text{Sel}^{(\psi)}(E'_1/\mathbb{Q})$. 由命题 3.5.1(1) 和 (2) 知 $d \mid n$ 且 $d \equiv \pm 1 \bmod 8$. 由命题 3.5.1(3) 知 $A\overrightarrow{v}(d) = \overrightarrow{0}$. 因此 $\overrightarrow{v}(d) = \overrightarrow{0}$ 或 $\overrightarrow{1}$, $d = \pm 1$ 或 $\pm n$. □

3.6 Selmer 群的像 $\widetilde{\text{Sel}}^{(\varphi)}$ 和 $\widetilde{\text{Sel}}^{(\psi)}$

令 $(a, b) = (a_1 n, b_1 n^2)$, 其中 $a_1, b_1 \in \mathbb{Z}$, b_1 最多只含素因子 2. 令 $E = E_{a,b}$, $d \in \text{Sel}^{(\varphi)}(E/\mathbb{Q})$. 我们希望找到 $d \in \widetilde{\text{Sel}}^{(\varphi)}(E/\mathbb{Q})$ 的必要条件.

设 $d = \tau^2 - b_1\mu^2$, 将引理 3.3.3中的 (σ, τ, μ) 取成 $(d, \tau + \frac{1}{2}a_1\mu, \frac{d\mu}{2n})$. 则(3.8)可以写成

$$\mathcal{M}_s : \begin{cases} w^2 = d\Big(\big(t^2 - a_1(nz^2/d)\big)^2 - 4b_1(nz^2/d)^2\Big), \\ w - \tau\big(t^2 - a_1(nz^2/d)\big) - 2b_1\mu(nz^2/d) = su^2. \end{cases} \tag{3.13}$$

命题 3.6.1. 假设 $d \in \mathrm{Sel}^{(\varphi)}(E/\mathbb{Q})$, $p \mid m$ 是奇素数. 若 $p \mid d$, 则 $\sqrt{b_1} \in \mathbb{Q}_p$. $\mathcal{M}_s$ 在 $p \mid m$ 处局部有解当且仅当:

(1) $p \mid d$, 选取 $\sqrt{b_1} \in \mathbb{Q}_p$ 使得 $p \mid \tau - \sqrt{b_1}\mu$,

$$p \mid s,\ \left(\frac{n/d}{p}\right) = \left(\frac{a_1 - 2\sqrt{b_1}}{p}\right), \quad \left(\frac{n/s}{p}\right) = \left(\frac{\mu}{p}\right),$$

或

$$p \nmid s,\ \left(\frac{n/d}{p}\right) = \left(\frac{a_1 + 2\sqrt{b_1}}{p}\right), \quad \left(\frac{s}{p}\right) = \left(\frac{-\mu}{p}\right)\left(\frac{n/d}{p}\right);$$

(2) $p \mid \frac{2m}{d}$,

$$p \mid s,\ \left(\frac{d}{p}\right) = \left(\frac{a_1^2 - 4b_1}{p}\right),\ \left(\frac{n/s}{p}\right) = \left(\frac{d}{p}\right)\left(\frac{\pm\sqrt{d(a_1^2 - 4b_1)} + a_1\tau - 2b_1\mu}{p}\right),$$

或

$$p \nmid s,\ \left(\frac{d}{p}\right) = 1,\ \left(\frac{s}{p}\right) = \left(\frac{\pm\sqrt{d} - \tau}{p}\right).$$

这里 $\pm$ 指取 $+$ 或 $-$ 均可.

证明. $p \mid d$ **的情形.** 不妨设 $z = 1, v(t) = 0, v(w) > 0$. 则 $t^2 \equiv (a_1 \pm 2\sqrt{b_1})\frac{n}{d} \bmod p$.

(i) 若 $v(su^2) \geq 3$, 则通过比较 w^2 的两个表达式, 我们得到

$$\left(\mu(t^2 - \frac{a_1 n}{d}) + \frac{2n\tau}{d}\right)^2 = O(su^2).$$

于是

$$t^2 \equiv \frac{(a_1\mu - 2\tau)n}{d\mu} \equiv (a_1 - 2\sqrt{b_1})\frac{n}{d} \bmod p, \quad \left(\frac{n/d}{p}\right) = \left(\frac{a_1 - 2\sqrt{b_1}}{p}\right).$$

令 $\beta = t^2 - \frac{(a_1\mu - 2\tau)n}{d\mu}$, 则

$$w^2 = d\left(\frac{4\tau^2 n^2}{\mu^2 d^2} - \frac{4n\tau\beta}{d\mu} + \beta^2 - 4b_1(\frac{n}{d})^2\right) = \frac{4n^2}{\mu^2}(1 - \frac{\tau\mu\beta}{n} + \frac{d\mu^2\beta^2}{4n^2}).$$

两边开根号得到

$$w = \pm\left(\frac{2n}{\mu} - \tau\beta - b_1 n\mu(\frac{\mu\beta}{2n})^2 + O(\beta^3/p^2)\right).$$

另一方面, $w = -\frac{2n}{\mu} + \tau\beta + su^2$, 因此这个符号只能取 $-$, 且 $su^2 = b_1 n\mu(\frac{\mu\beta}{2n})^2 + O(\frac{\beta^3}{p^2})$, 于是 $p \mid s$, $\left(\frac{n/s}{p}\right) = \left(\frac{\mu}{p}\right)$.

(ii) 若 $v(bu^2) \leq 2$ 且 $t^2 \equiv \frac{(a_1 - 2\sqrt{b_1})n}{d} \bmod p$, 则 $\left(\frac{n/d}{p}\right) = \left(\frac{a_1 - 2\sqrt{b_1}}{p}\right)$. 令

$$t^2 = \frac{(a_1 - 2\sqrt{b_1})n}{d} - \frac{p^2\alpha}{n\sqrt{b_1}},$$

则

$$w^2 = 4p^2\alpha(1+\frac{p^2d\alpha}{4n^2b_1}),$$

$$w = \pm 2p\sqrt{\alpha}(1+\frac{p^2d\alpha}{8n^2b_1}+O(p^2)),$$

$$su^2 = \frac{p^2\tau}{n\sqrt{b_1}}(\sqrt{\alpha}\pm\frac{n\sqrt{b_1}}{p\tau})^2+\frac{n\sqrt{b_1}}{d\tau}(\tau-\sqrt{b_1}\mu)^2\pm\frac{p^3d}{4n^2b_1}\alpha^{3/2}+O(p^3).$$

如果 $v(su^2)=2$, 则 $\sqrt{\alpha}\equiv\mp\frac{n\sqrt{b_1}}{p\tau}$ mod p,

$$su^2 = \frac{n\sqrt{b_1}}{4d\tau^3}(\tau-\sqrt{b_1}\mu)^3(3\tau+\sqrt{b_1}\mu)+O(p^3)=O(p^3),$$

这不可能. 因此 $v(su^2)=1, p\mid s$, $\left(\frac{n/s}{p}\right)=\left(\frac{\tau\sqrt{b_1}}{p}\right)=\left(\frac{\mu}{p}\right)$.

(iii) 若 $v(su^2)\le 2$ 且 $t^2\equiv\frac{(a_1+2\sqrt{b_1})n}{d}$ mod p, 则 $\left(\frac{n/d}{p}\right)=\left(\frac{a_1+2\sqrt{b_1}}{p}\right)$,

$$su^2 = -2\sqrt{b_1}\tau n/d-2b_1\mu n/d+O(p)=-4b_1n\mu/d+O(p),$$

于是 $p\nmid s$, $\left(\frac{s}{p}\right)=\left(\frac{-\mu}{p}\right)\left(\frac{n/d}{p}\right)$.

$p\mid\frac{2m}{d}$ 的情形.

(i) 若 $v(z)\ge v(t)=v(w)/2$, 不妨设 $t=1, v(w)=0, v(z)\ge 0$, 则 $\left(\frac{d}{p}\right)=1$ 且

$$\begin{aligned} w &= \pm\sqrt{d}(1-a_1(nz^2/d)-2b_1(nz^2/d)^2+\cdots)\\ &= \tau-(a_1\tau+2b_1\mu)\frac{nz^2}{d}+su^2. \end{aligned}$$

注意到 $(\sqrt{d}-\tau)(-\sqrt{d}-\tau)=b_1\mu^2$ 和 $\pm\sqrt{d}-\tau$ 互素. 选择合适的 $\sqrt{d}$ 或 τ 使得 $\sqrt{d}-\tau\ne 0$, 则 $v(\sqrt{d}-\tau)$ 是偶数, 于是 $\left(\frac{\sqrt{d}-\tau}{p}\right)$ 是良定的.

不妨设 $p\nmid(\sqrt{d}+\tau)$. 若 $w\equiv-\sqrt{d}$ mod p 或 $p\nmid\mu$, 则 $su^2=-\sqrt{d}-\tau+O(p)$. 若 $w\equiv\sqrt{d}$ mod p, 则 $v(\mu)\ge 1$,

$$b_1\Big(\mu(1-\frac{a_1nz^2}{d})+2\tau\frac{nz^2}{d}\Big)^2=-su^2(2\tau+O(p)),$$

因此 $p\nmid s$, $\left(\frac{s}{p}\right)=\left(\frac{-2\tau}{p}\right)=\left(\frac{\pm\sqrt{d}-\tau}{p}\right)$.

(ii) 若 $v(z)<v(t)$, 不妨设 $z=1, w=pw_1, t=pt_1$, 则

$$w_1^2=(a_1^2-4b_1)d(\frac{n}{pd})^2+O(p),$$

因此 $\left(\frac{d}{p}\right)=\left(\frac{a_1^2-4b_1}{p}\right)$,

$$w_1=\pm\sqrt{(a_1^2-4b_1)d}(\frac{n}{pd})+O(p),$$

$$su^2 = \frac{n}{d}(a_1\tau - 2b_1\mu \pm \sqrt{(a_1^2 - 4b_1)d} + O(p)).$$

注意到

$$(a_1\tau - 2b_1\mu + \sqrt{(a_1^2 - 4b_1)d})(a_1\tau - 2b_1\mu - \sqrt{(a_1^2 - 4b_1)d}) = b_1(a_1\mu - 2\tau)^2.$$

因此

$$p \mid s, \quad \left(\frac{n/s}{p}\right) = \left(\frac{d}{p}\right)\left(\frac{a_1\tau - 2b_1\mu \pm \sqrt{(a_1^2 - 4b_1)d}}{p}\right). \qquad \square$$

3.7 估计 $\widetilde{\text{Sel}}^{(\varphi)}$

对于 E_i, $(a_1, b_1) = (0, -1), (3, 2)$ 或 $(-3, 2)$.

推论 3.7.1. *设 $d \in \text{Sel}^{(\varphi_i)}(E_i/\mathbb{Q})$, $p \mid m$ 是奇素数. 令 $d = \tau^2 - b_1\mu^2$, 假设对所有的 p, $\left(\frac{b_1}{p}\right) = 1$ 且 $\left(\frac{-a_1+2\sqrt{b_1}}{p}\right) = \left(\frac{-a_1-2\sqrt{b_1}}{p}\right) = 1$. 选取 $\sqrt{b_1} \in \mathbb{Z}/m\mathbb{Z}$ 使得 $p \mid \tau - \sqrt{b_1}\mu$ 对任意 $p \mid d'$ 成立, 则 $\mathcal{M}_s$ 在 p 处有解仅当*

(1) $p \mid d'$,

$$p \mid s, \ \left(\frac{n/d}{p}\right) = \left(\frac{-1}{p}\right), \ \left(\frac{n/s}{p}\right) = \left(\frac{-2(\tau + \sqrt{b_1}\mu)}{p}\right)\left(\frac{-\sqrt{b_1}}{p}\right);$$
$$p \nmid s, \ \left(\frac{n/d}{p}\right) = \left(\frac{-1}{p}\right), \ \left(\frac{s}{p}\right) = \left(\frac{-2(\tau + \sqrt{b_1}\mu)}{p}\right)\left(\frac{-\sqrt{b_1}}{p}\right);$$

(2) $p \mid \frac{m}{d'}$,

$$p \mid s, \ \left(\frac{d}{p}\right) = 1, \ \left(\frac{n/s}{p}\right) = \left(\frac{-2(\tau + \sqrt{b_1}\mu)}{p}\right);$$
$$p \nmid s, \ \left(\frac{d}{p}\right) = 1, \ \left(\frac{s}{p}\right) = \left(\frac{-2(\tau + \sqrt{b_1}\mu)}{p}\right).$$

特别地, 若 E_i 为定理 3.2.1(1) 中的 E_1 或 (3) 中的 E_3, 则

$$\left[\frac{-\sqrt{b_1}}{d'}\right] + \left[\frac{-2(\tau + \sqrt{b_1}\mu)}{m}\right] = 1 \implies d \notin \widetilde{\text{Sel}}^{(\varphi)}(E_i/\mathbb{Q}).$$

证明. 若 $p \mid d$,

$$\left(\frac{\mu}{p}\right) = \left(\frac{4b_1\mu}{p}\right) = \left(\frac{-\sqrt{b_1}}{p}\right)\left(\frac{-2(\tau + \sqrt{b_1}\mu)}{p}\right).$$

若 $p \mid \frac{n}{d}$, 如果 $p \nmid s$, 则

$$-2(\sqrt{d} - \tau)(\tau + \sqrt{b_1}\mu) = (\tau + \sqrt{b_1}\mu - \sqrt{d})^2, \tag{3.14}$$

$$\left(\frac{s}{p}\right)=\left(\frac{-2(\tau+\sqrt{b_1}\mu)}{p}\right).$$

若 $p\mid s$, 注意到 $(a_1^2-4b_1)d=(-a_1\tau+2b_1\mu)^2-b_1(2\tau-a_1\mu)^2$,

$$\left(\frac{n/s}{p}\right)=\left(\frac{-2(-a_1\tau+2b_1\mu+\sqrt{b_1}(2\tau-a_1\mu))}{p}\right)=\left(\frac{-2(\tau+\sqrt{b_1}\mu)}{p}\right).$$

其余由命题 3.6.1可得.

若 $E_i=E_1$, $(a_1,b_1)=(0,-1)$, 对任意 $p\mid d$, $p\equiv 1 \bmod 4$, $\left(\frac{2\sqrt{-1}}{p}\right)=1$; 若 $E_i=E_3$, $(a_1,b_1)=(-3,2)$, 对任意 $p\mid d$, $p\equiv \pm 1 \bmod 8$, $\left(\frac{3\pm 2\sqrt{2}}{p}\right)=1$. 如果 $d\in \tilde{S}^{(\varphi_i)}(E_i/\mathbb{Q})$, 则存在 $s\in\mathbb{Q}(S,2)$ 满足上述条件. 令 $\varepsilon=s/d(\overrightarrow{v}(s))=\pm 1,\pm 2$, 则

$$A\overrightarrow{v}(s)\text{ 的第}i\text{ 个分量}=\begin{cases}\left[\frac{-2(\tau+\sqrt{b_1}\mu)}{p}\right]+\left[\frac{-\sqrt{b_1}}{p}\right]+\left[\frac{\varepsilon}{p}\right], & \text{若 } p_i\mid d;\\ \left[\frac{-2(\tau+\sqrt{b_1}\mu)}{p}\right]+\left[\frac{\varepsilon}{p}\right], & \text{若 } p_i\mid \frac{m}{d}.\end{cases}$$

由于矩阵 A 的像空间是 $x_1+\cdots+x_k=0$ 的子空间, 且 $m\equiv 1 \bmod 8, \sum\left[\frac{\varepsilon}{p}\right]=\left[\frac{\varepsilon}{m}\right]=0$, 因此

$$\left[\frac{-\sqrt{b_1}}{d'}\right]+\left[\frac{-2(\tau+\sqrt{b_1}\mu)}{m}\right]=0. \qquad \square$$

3.8　主定理的证明

定理 3.2.1的证明. (1) 由推论 3.5.2(1),

$$\mathrm{Sel}^{(\varphi)}(E_1/\mathbb{Q})=\{1,n,2d,2n/d\},\ \mathrm{Sel}^{(\psi)}(E_1'/\mathbb{Q})=\{\pm 1,\pm n\},$$

其中 $d=d(\overrightarrow{v})$, $A\overrightarrow{v}=C_2\overrightarrow{1}$. 令 $2d=\tau^2+\mu^2$, 选取合适的 $\sqrt{-1}\in\mathbb{Z}/n\mathbb{Z}$ 使得对任意奇素数 $p\mid d$, $p\mid \tau-\sqrt{-1}\mu$. 由推论 3.7.1, 如果 $\left[\frac{\tau+\sqrt{-1}\mu}{n}\right]+\left[\frac{2}{d}\right]=1$, 则 $2d\notin \widetilde{\mathrm{Sel}}^{(\varphi)}(E_1/\mathbb{Q})$. 由命题 3.4.1, $\widetilde{\mathrm{Sel}}^{(\varphi)}(E_1/\mathbb{Q})=\{1\}$ 且 n 是非同余数.

(2) 若 $n=m$ 是奇数, 由推论 3.5.2(2),

$$\mathrm{Sel}^{(\varphi)}(E_3/\mathbb{Q})=\{1,d,-n,-n/d\},\ \mathrm{Sel}^{(\psi)}(E_3'/\mathbb{Q})=\{1,2,n,2n\}$$

其中 $d=d(\overrightarrow{v}),\overrightarrow{v}\neq 0,(A+C_{-1})\overrightarrow{v}=\overrightarrow{0}$. 令 $-n=\tau^2-2\mu^2$, 由 $m\equiv 1 \bmod 8$ 知 μ 是奇数. 选取合适的 $\sqrt{2}$ 使得对任意奇素数 $p\mid n, p\mid \tau-\sqrt{2}\mu$. 则

$$\left[\frac{-\sqrt{2}}{n}\right]+\left[\frac{-2(\tau+\sqrt{2}\mu)}{n}\right]=\left[\frac{\mu}{n}\right]=\left[\frac{n}{|\mu|}\right]=\left[\frac{-1}{|\mu|}\right].$$

由推论 3.7.1, $|\mu|\equiv 3 \bmod 4$ 推出 $-n\notin \widetilde{\mathrm{Sel}}^{(\varphi)}(E_3/\mathbb{Q})$. 由命题 3.4.1, $\widetilde{\mathrm{Sel}}^{(\varphi)}(E_3/\mathbb{Q})=\{1\}$ 且 n 是非同余数.

若 $n=2m$ 是偶数, 由推论 3.5.2(2),

$$\text{Sel}^{(\varphi)}(E_3/\mathbb{Q})=\begin{cases}\{1,2,d,2d\}, & \text{若 } d\equiv 1 \bmod 8;\\ \{1,2,-m/d,-n/d\}, & \text{若 } d\equiv -1 \bmod 8\end{cases}$$

且 $\text{Sel}^{(\psi)}(E_3'/\mathbb{Q})=\{1,2,m,n\}$, 其中 $d=d(\overrightarrow{v}),\overrightarrow{v}\neq 0,(A+C_{-1})\overrightarrow{v}=\overrightarrow{0}$. 取 $\tau=2,\mu=1,2=2^2-2\times 1^2$, 则 $\left[\frac{-2(2+\sqrt{2})}{m}\right]=\left[\frac{2+\sqrt{2}}{m}\right]$. 由推论 3.7.1, $\left(\frac{2+\sqrt{2}}{m}\right)=-1$ 推出 $2\notin\widetilde{\text{Sel}}^{(\varphi)}(E_3/\mathbb{Q})$. 由命题 3.4.1, $\widetilde{\text{Sel}}^{(\varphi)}(E_3/\mathbb{Q})=\{1\}$ 且 n 是非同余数. □

注 3.8.1. 令 E 为定理 *3.2.1*(1) 的 E_1 或 (2) 的 E_3, 则

$$\text{rank}\,E(\mathbb{Q})=0,\quad Ш(E/\mathbb{Q})[2^\infty]\cong(\mathbb{Z}/2\mathbb{Z})^2. \tag{3.15}$$

第四章　函数域上的 Birch 引理

本章基于我们的论文 [OuZ3].

4.1　记号和结论

设 F 为特征 $p>0$ 的整体函数域, 其常数域为 q 阶有限域 $\mathbb{F}_q$, 即 $\mathbb{F}_q$ 是包含在 F 中的最大的有限域. 固定 F 的一个素位 ∞, 记 $\mathcal{O}_F$ 为 F 上在 ∞ 以外的素位均正规的元素构成的集合. 令 F_∞ 为 F 在 ∞ 的完备化, C 为 F_∞ 的代数闭包的完备化.

回忆 Atkin–Lehner 算子在带 N 循环子群 Z 的 Drinfeld 模 D 的作用如下:

$$w_N=\prod_{\mathfrak{p}|N} w_{\mathfrak{p}},$$

$$w_{\mathfrak{p}}(D,Z)=(D/Z_{\mathfrak{p}^k},(D_{\mathfrak{p}^k}+Z)/Z_{\mathfrak{p}^k}),\quad \mathfrak{p}^k\parallel N.$$

令 d_N 为 N 在理想类群 $\mathrm{Pic}(\mathcal{O}_F)$ 中的阶, 则 w_N 的阶为 $2d_N$ 且 $w=w_N^{d_N}$ 为对合.

令 (E,O) 为 F 上椭圆曲线. 假设 E 在 ∞ 处有分裂的乘性约化, 导子为 $N_E=N\infty$. 由函数域上椭圆曲线的模性, 存在 F 上非常值映射

$$f: X_0(N)\to E.$$

固定 O 的一个原像 $P_0\in f^{-1}(O)$.

设 $l\in\mathcal{O}_F$ 无平方因子且不是常数, 设虚二次扩张 $K=F(\sqrt{l})/F$ 在 ∞ 处分歧, 则 $K\neq F\otimes_{\mathbb{F}_q}\mathbb{F}_{q^2}$. 令 τ 为 $\mathrm{Gal}(K_\infty/F_\infty)$ 中非平凡元素. 我们将 K 中 ∞ 分歧得到的素位仍记做 ∞.

从现在起, 我们假设

(I) $f(P_0^w)\notin 2E(F)$.

(II) $\mathcal{O}_K$ 的类数 $h=h(\mathcal{O}_K)$ 是奇数.

(III) (Heegner 假设) 任一素因子 $\mathfrak{p}\mid N$ 在 $\mathcal{O}_K$ 中分裂, 由此我们可以分解 $N\mathcal{O}_K=\mathfrak{N}\mathfrak{N}^\tau$, 其中 $\mathfrak{N}$ 是 $\mathcal{O}_K$ 中理想.

(IV) $\mathfrak{M}=\mathfrak{q}_1\cdots\mathfrak{q}_r$ 是 F 中不同的有限素理想的乘积, 其中 E 在 $\mathfrak{q}_i$ 处有好约化, Fourier 系数 $a_{\mathfrak{q}_i}=0$, $\mathfrak{q}_i$ 与 N 互素, 在 K 中惯性, 且剩余域 $\kappa(\mathfrak{q}_i)$ 的大小 $\equiv 1 \bmod 4$ (因此 $p\neq 2$).

对于 $\mathcal{O}_K$ 的理想 $\mathfrak{d}$, 令 $\mathcal{O}_\mathfrak{d}=\mathcal{O}_F+\mathfrak{d}$ 为导子为 $\mathfrak{d}$ 的**序模**, $\mathcal{O}_{\mathfrak{d},v}$ 为 $\mathcal{O}_\mathfrak{d}$ 在 v 处的完备化. 由类域论知,

$$K^\times\prod_{v\neq\infty}\mathcal{O}_{\mathfrak{d},v}^\times$$

对应 K^{ab}/K 的子扩张 $H_{\mathfrak{d}}$, 称为对应 $\mathfrak{d}$ 的 K 的**环类域**. 特别地, 令 $H_K := H_1$ 是 K 的 Hilbert 类域. $H_{\mathfrak{d}}$ 在 $v \mid \mathfrak{d}$ 处完全分歧, 在 ∞ 处完全分裂, 在其它素位不分歧, 因此我们可以将 $H_{\mathfrak{d}}$ 嵌入到 K_∞.

引理 4.1.1. *设 d_i 为 $[\mathfrak{q}_i]$ 在 $\mathcal{O}_F$ 的理想类群 $\mathrm{Pic}(\mathcal{O}_F)$ 中的阶. 则 $H_{\mathfrak{q}_i}$ 包含唯一的一个 K 的二次扩张 $K(\sqrt{c_i})$, 其中 $c_i \in \mathcal{O}_F$ 是 $\mathfrak{q}_i^{d_i}$ 的一个生成元使得 c_i 在 $\kappa(\infty)$ 的像是个平方.*

证明. 由 [Bro, (2.3.8)], Galois 群

$$\mathrm{Gal}(H_{\mathfrak{q}_i}/H_K) = \frac{(\mathcal{O}_K/\mathfrak{q}_i\mathcal{O}_K)^\times}{(\mathcal{O}_F/\mathfrak{q}_i)^\times}$$

的大小为 $\#\kappa(\mathfrak{q}_i)+1$. 由假设 (II) 和 (IV), $[H_{\mathfrak{q}_i} : K]$ 的大小模 4 余 2, 因此这个域扩张包含唯一的一个二次子扩张.

由于 ∞ 在 K 中分歧, K_∞ 和 F_∞ 的剩余域相同. 由于 h 是奇数, F 上 ∞ 的次数也是奇数. 我们断言 d_i 是奇数. 若不然, 令 $I = \mathfrak{q}_i^{d_i/2}$, 则由假设 (II), h 是奇数, 于是 $I\mathcal{O}_K$ 是主理想. 令 $I\mathcal{O}_K = (a), I^2 = (b)$, 则存在 $\varepsilon \in \mathbb{F}_q^\times$ 使得 $a^2 = b\varepsilon$, 且 $K = F(\sqrt{b\varepsilon})$. 而 $b\varepsilon$ 在 ∞ 处的赋值为偶数, 这与 ∞ 在 K 上分歧矛盾.

令 c 为 $\mathfrak{q}_i^{d_i}$ 的一个生成元. 则 $\mathfrak{q}_i$ 是 $K(\sqrt{c})/K$ 中唯一一个分歧的有限素位. 若 $K(\sqrt{c'})$ 是另一个 K 的二次扩张, 满足 $\mathfrak{q}_i$ 是其中唯一一个分歧的有限素位, 则 c'/c 在每个素位的赋值都是偶数, 即存在 $\mathcal{O}_K$ 中的分式理想 J 使得 $(c'/c)\mathcal{O}_K = J^2$. 由于 h 是奇数, J 是主理想, 从而 $K(\sqrt{c'}) = K(\sqrt{c})$ 或 $K(\sqrt{\varepsilon c})$, 其中 $\varepsilon \in \mathbb{F}_q - \mathbb{F}_q^2$. 因此 $H_{\mathfrak{q}_i}/K$ 中唯一的二次子扩张可以写成 $K(\sqrt{c_i})$, 其中 c_i 是 $\mathfrak{q}_i^{d_i}$ 的一个生成元.

由于 $c_i \in K_\infty^2$, 这等价于 c_i 在 $\kappa(\infty)$ 中的像是个平方. 由此我们在相差 $\mathbb{F}_q^{\times 2}$ 的意义下唯一决定了 c_i. □

令

$$q_i = \begin{cases} c_i, & \text{若 } \tau(\sqrt{c_i}) = \tau(\sqrt{c_i}); \\ c_i l, & \text{若 } \tau(\sqrt{c_i}) = -\tau(\sqrt{c_i}). \end{cases} \tag{4.1}$$

则 $\tau(\sqrt{q_i}) = \sqrt{q_i}$ 且 $K(\sqrt{q_i}) = K(\sqrt{c_i})$.

我们还假设:

(V) q_i 是模 N 的平方. (如果 N 是平方数, 该条件自动成立.)

令 $M = \prod_{i=1}^r q_i$. 则我们的函数域版本的 Birch 引理为:

定理 4.1.2. *假设 $(I)-(V)$, 则 $E(F(\sqrt{lM}))^-$ 无限. 更进一步, 若 $E^{(lM)}$ 是 E 关于 lM 的二次扭, 则 $E^{(lM)}(F)$ 秩为 1 且精确 BSD 猜想成立.*

这里 $^-$ 表示 $\tau = -1$ 的部分.

注 4.1.3. *在数域情形, 设 E 为 $\mathbb{Q}$ 上导子为 N 的椭圆曲线, $f : X_0(N) \to E$ 是模参数化. 假设 $f([0]) \notin 2E(\mathbb{Q})$, $l > 3$ 是模 4 余 3 的素数且任意素数 $p \mid N$ 在 $\mathbb{Q}(\sqrt{-l})$ 中分裂, 则 $E^{(-l)}(\mathbb{Q})$ 秩为 1.*

更进一步, 如果 E 存在超奇异好约化 q_1, 且 $q_1 \equiv 1 \mod 4$, N 是模 q_1 的平方. 则对任意给定的正整数 k, 存在无穷多平方自由的整数 M 恰有 k 个素因子, 使得

$L(E^{(M)},s)$ 在 $s=1$ 处阶为 1. 特别地, $E=X_0(14)$, $q_1=5$ 和 $E=X_0(49)$, $q_1=5$, 满足上述条件, 参见 [CLTZ, 定理 1.1].

在函数域情形, 若 $F=\mathbb{F}_q(t),\infty=1/t,E=X_0(N)$ 是椭圆曲线, 则 q 必须为 2 (参见 [Sch]), 这不满足我们的假设条件. 函数域情形由于没有 *Gauss* 亏格理论, 因此难以确定虚二次域的类数的奇偶性.

注 4.1.4. 如果 K 在 ∞ 处惯性, 则 ∞ 在 K 中的次数为偶数, $\mathcal{O}_K$ 的类数 $\deg(\infty)h(K)$ 一定是偶数, 这不满足我们的假设 (II).

注 4.1.5. 不同与数域情形, 即使 p 充分大, 条件 $a_{q_i}=0$ 也不能替换为 E 在 $\mathfrak{q}_i$ 处有超奇异约化.

引理 4.1.6. d_i 整除 h.

证明. 由于 $\mathfrak{q}_i\mathcal{O}_K$ 在 $\mathrm{Pic}(\mathcal{O}_K)$ 中的阶整除 d_i 和 h, 因此整除 $d_i=(d_i,h)$，从而 $(\mathfrak{q}_i\mathcal{O}_K)^{(d_i,h)}=(a)$ 是主理想. 设 $\mathfrak{q}_i^{d_i}=(b)$. 若 $d_i\nmid h$, 令 $\alpha=d_i/(d_i,h)$, 则 $a\in b^{1/\alpha}\mathbb{F}_q^\times$, 但是 $\alpha>2$, 这不可能. 因此原命题成立. □

由此, 我们可以将我们的结果改写为如下形式, 其中 lM 和 M' 相差一个平方数.

定理 4.1.7. 假设 $(I)-(V)$, 设 M_0 是 $\mathfrak{M}^h$ 的一个生成元使得 M_0 的像是 $\kappa(\infty)$ 中的平方, $M'=M_0$ 或 lM_0 满足 $\tau(\sqrt{M'})=-\sqrt{M'}$, 则 $E(F(\sqrt{M'}))^-$ 无限. 更进一步, $E^{(M')}(F)$ 秩为 1 且精确 *BSD* 猜想成立.

4.2 Heegner 点和 Atkin–Lehner 算子

设 $\mathcal{O}_\mathfrak{M}=\mathfrak{M}+\mathcal{O}_F$ 是 K 中导子为 $\mathfrak{M}$ 的序模, $\mathfrak{a}$ 是它的理想, $\mathfrak{N}_\mathfrak{M}=\mathfrak{N}\cap\mathcal{O}_\mathfrak{M}$. 定义 Heegner 点

$$P_{\mathfrak{a},\mathfrak{N},\mathfrak{M}}:=(C/\mathfrak{a}\to C/\mathfrak{a}\mathfrak{N}_\mathfrak{M}^{-1})\in X_0(N)(H_\mathfrak{M}).$$

Galois 群在 Heegner 点集上的作用为

$$P_{\mathfrak{a},\mathfrak{N},\mathfrak{M}}^{[\alpha,H_\mathfrak{M}/K]}=P_{\mathfrak{a}\alpha^{-1},\mathfrak{N},\mathfrak{M}},\tag{4.2}$$

其中 $[-,H_\mathfrak{M}/K]$ 是 Artin 符号, 参见 [Bro, §4.5].

Atkin–Lehner 算子 w_N 在 Heegner 点上的作用为

$$w_NP_{\mathfrak{a},\mathfrak{N},\mathfrak{M}}=P_{\mathfrak{a}\mathfrak{N}^{-1},\mathfrak{N}^\tau,\mathfrak{M}}.\tag{4.3}$$

我们将 $P_{\mathcal{O}_\mathfrak{M},\mathfrak{N},\mathfrak{M}}$ 简记为 $P_\mathfrak{M}$, 则

$$\tau P_\mathfrak{M}^{[\mathfrak{N}^{-1},H_\mathfrak{M}/K]}=w_N(P_\mathfrak{M}).\tag{4.4}$$

令 $H_0=K(\sqrt{q_1},\dots,\sqrt{q_r})$, 它是 $H_\mathfrak{M}$ 的子域且 $[H_\mathfrak{M}:H_0]$ 是奇数.

引理 4.2.1. 令 S 为 $P_{\mathfrak{M}}$ 在 $\mathrm{Gal}(H_{\mathfrak{M}}/H_0)$ 作用下的轨道, 则 $w_N S = \tau S$.

证明. $[\mathfrak{N}, H_{\mathfrak{M}}/K]$ 限制在 $F(\sqrt{q_i})$ 的作用等于 $[N\mathcal{O}_F, F(\sqrt{q_i})/F]$. 根据假设 (V), 它固定了 $\sqrt{q_i}$. □

引理 4.2.2. $f + f \circ w$ 是常数.

证明. 令 $J_0(N) = \mathrm{Jac}(X_0(N))$, $A = J_0(N)/(T_n - a_n; n \nmid N)$. 由模映射的构造可知, 我们可以将 f 写成

$$\begin{aligned} X_0(N) &\to J_0(N) \\ P &\mapsto [P] - [P_0], \end{aligned}$$

与如下映射的复合

$$g : J_0(N) \to A, \quad h : A \to E,$$

这里 T_n 是 n 次 Hecke 算子, a_n 为 E 的第 n 个 Fourier 系数, h 是一个同源. 令 $f_A : P \mapsto g([P] - [P_0])$ 为前两个映射的复合.

由定义, w 是 $J_0(N)$ 上的对合, 且

$$w([P] - [P_0]) = [P^w] - [P_0^w].$$

由于 w 和 T_n 交换, 因此 w 诱导了 A 上的对合 $w = \pm 1$.

若 $w = +1$, 则

$$\begin{aligned} &(f_A - f_A \circ w)(P) \\ =&w(f_A - f_A \circ w)(P) \\ =&w \circ g(([P] - [P_0]) - ([P^w] - [P_0])) \\ =&w \circ g([P] - [P^w]) \\ =&g([P^w] - [P]) \\ =&(f_A \circ w - f_A)(P). \end{aligned}$$

$f_A - f_A \circ w$ 的像落在 $A[2]$, 这是个有限集. 因此 $f_A - f_A \circ w$ 是常数.

类似引理4.1.1可知 N 的阶 d_N 是奇数. 由于 F 上 ∞ 的阶是奇数, F_∞ 不包含 $\mathbb{F}_{q^2}$. 我们可以选取 $c \in C - F_\infty$ 使得 c^2 生成 N^{d_N}. 记 $d_N = 2t + 1$. 令

$$\Lambda = N + N^{-t}c^{-1}, \Lambda' = A + N^{-t}c^{-1},$$

则

$$\begin{aligned} &w(C/\Lambda \to C/\Lambda') \\ =&(C/N^{-t}\Lambda' \to C/N^{-t-1}\Lambda) \\ =&(C/(N^{-t} + N^{-2t}c^{-1}) \to C/(N^{-t} + Ac)) \\ =&(C/(N^{-t}c^{-1} + N^{-2t}c^{-2}) \to C/(N^{-t}c^{-1} + A)) \\ =&(C/\Lambda \to C/\Lambda') \in X_0(N). \end{aligned}$$

也就是说, $Q = (C/\Lambda \to C/\Lambda')$ 是 w 的一个不动点. 于是

$$f_A(P_0^w) = f_A(P_0^w) - f_A(P_0) = f_A(Q^w) - f_A(Q) = O$$

且 $f(P_0^w)=O$, 这与假设 (I) 矛盾. 因此 $w=-1$.

一方面,

$$2g([P]+[P^w]-[P_0]-[P_0^w])=f_A(P)+f_A(P^w)+wf_A(P)+wf_A(P^w)=0.$$

另一方面,

$$\begin{aligned}&g([P]+[P^w]-[P_0]-[P_0^w])\\=&(f_A+f_A\circ w)(P)-g([P_0^w]-[P_0])\\=&(f_A+f_A\circ w)(P)-f_A(P_0^w).\end{aligned}$$

因此 $f_A+f_A\circ w$ 的像落在 $f_A(P_0^w)+A[2]$, 这是个有限集. 因此 $f_A+f_A\circ w$ 是常数且 $f+f\circ w=f(P_0^w)$. □

注 4.2.3. 容易看出假设 (I) 等价于对某一个 (或任意) P, 有 $f(P)+f(P^w)\notin 2E(F)$.

现在, $f(P_{\mathfrak{M}})$ 是一个 Heegner 点, 我们将要将它降至更小的域, 同时, 我们还需要证明得到的点是无限阶点.

命题 4.2.4. $y_0=\mathrm{Tr}_{H_{\mathfrak{M}}/H_0}f(P_{\mathfrak{M}})$ 是无限阶点.

证明. 由引理4.2.1, 4.2.2, 我们有

$$P_{\mathfrak{M}}+\tau(P_{\mathfrak{M}})=f(P_0^w), \tag{4.5}$$

$$y_0+\tau(y_0)=[H_{\mathfrak{M}}:H_0]f(P_0^w). \tag{4.6}$$

由于对于 H_0 的任一严格包含 F 的子域, 至少有一个整除 $l\mathfrak{q}_1\cdots\mathfrak{q}_r$ 的素位分歧. 但是 $F(E[2^\infty])$ 只有 $2N\infty$ 的因子才可能分歧, 因此有

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

若 y_0 是有限阶, 则存在奇数 t 使得

$$ty_0\in E(H_0)[2^\infty]=E(F)[2^\infty].$$

由于 $[H_{\mathfrak{M}}:H_0]$ 是奇数,

$$f(P_0^w)=([H_{\mathfrak{M}}:H_0]t+1)f(P_0^w)-2ty_0\in 2E(F),$$

这与假设 (I) 矛盾. □

4.3　欧拉系

对于 $\mathfrak{M}$ 的因子 $\mathfrak{d}$, 令 $d=\prod_{\mathfrak{q}_i|\mathfrak{d}}q_i$. 定义 E 的 $K(\sqrt{d})$ 点 y_d:

$$y_d=\sum_{\sigma\in\mathrm{Gal}(H_{\mathfrak{M}}/K)}\chi_d(\sigma)f(P_{\mathfrak{M}})^\sigma=\sum_{\sigma\in\mathrm{Gal}(H_0/K)}\chi_d(\sigma)y_0^\sigma. \tag{4.7}$$

回忆 a_v 是 E 在 v 处的 Fourier 系数, 根据 [Bro, (4.6.8)], 我们有如下欧拉系:

命题 4.3.1. *对于 $\mathfrak{q}_i \mid \frac{\mathfrak{M}}{\mathfrak{d}}$, 我们有*

$$\mathrm{Tr}_{H_{\mathfrak{q}_i\mathfrak{d}}/H_{\mathfrak{d}}} f(P_{\mathfrak{q}_i\mathfrak{d}}) = a_{\mathfrak{q}_i} f(P_{\mathfrak{d}}) = 0.$$

由此对任意 $\mathfrak{d} \neq \mathfrak{M}$, $y_d = 0$.

回顾 Tate, Milne, Kato 和 Trihan 等人的定理, 参见 [Vig, 定理 7.2].

定理 4.3.2. *以下三条等价:*

(1) *E/F 的精确 BSD 猜想成立.*

(2) *E/F 的 Tate–Shafarevich 群有限.*

(3) *设 l 是素数, E/F 的 Tate–Shafarevich 群的 l 部分有限.*

定理4.1.2的证明. 由 y_d 的定义知

$$y_M + \sum_{\mathfrak{d}\mid\mathfrak{M},\mathfrak{d}\neq\mathfrak{M}} y_d = 2^r y_0,$$

于是 $y_M = 2^r y_0$. 设 s 是 $f(P_0^w)$ 的阶, $y = s y_M$.

假设 $\sigma \in \mathrm{Gal}(H_0/K)$ 将 $\sqrt{q_i}$ 映为 $-\sqrt{q_i}$ 而保持 $\sqrt{q_j}, j \neq i$ 不动, 则

$$\sigma(y_0) + y_0 = \mathrm{Tr}_{H_{\mathfrak{M}}/K(\sqrt{q_j}, j\neq i)} f(P_M).$$

该扩张有中间域 $H_{\mathfrak{M}/\mathfrak{q}_i}$, 根据命题4.3.1, 我们有

$$\sigma(y_0) + y_0 = 0.$$

因此

$$\sigma(y) + y = 0.$$

同时由方程(4.6)知 $\tau(y) + y = 0$, 因此 $y \in E(F(\sqrt{lM}))^-$.

由于 y_0 是无限阶点, 因此 y 也是.

类似于 [Vig, 定理 7.1] 的证明, 我们取一个充分大的素数 t, 令 $\chi = \chi_M$, 则 Selmer 群之间有如下关系

$$\mathrm{Sel}^{(t)}(E/F(\sqrt{lM}))^\chi \hookrightarrow \mathrm{Sel}^{(t)}(E/K(\sqrt{M}))^\chi \hookrightarrow \mathrm{Sel}^{(t)}(E/H_{\mathfrak{M}})^\chi.$$

由 [Vig, 定理 6.1] 知最后一项的 $\mathbb{F}_t$ 秩为 1. 令

$$\delta : E(F(\sqrt{lM}))^- \to \mathrm{Sel}^{(t)}(E/F(\sqrt{lM}))^\chi$$

为 Kummer 映射, 则 $\mathrm{Sel}^{(t)}(E/F(\sqrt{lM}))^\chi$ 包含非零元 δy, 由此可知这些 Selmer 群的 $\mathbb{F}_t$ 秩均为 1.

我们知道 $E^{(lM)}(F) \cong E(F(\sqrt{lM}))^-$. 由限制映射是单射可知,

$$\dim_{\mathbb{F}_t} \text{Sel}_t(E^{(lM)}/F) = 1, \quad Ш\,(E^{(lM)}/F)[t] = 0.$$

由定理 4.3.2 知这蕴含 $E^{(lM)}/F$ 的精确 BSD 猜想成立. □

第五章　展望

本章我们将讨论和展望更一般的秩零或秩一情形的 BSD 猜想.

5.1　同余数问题

利用 2 下降法寻找非同余数的方法最早来自 Fermat, 这种寻找非同余数的方式本质上是计算 Selmer 群的大小并利用 Selmer 群的大小来限制同余椭圆曲线的秩, 这就导致了它的 Tate–Shafarevich 群的 2 部分不能太大. 而从王章杰 [王] 的结果我们可以看出, 这种寻找非同余数所需的条件已经十分复杂. 根据 Coates–Wiles [CoW] 的结果, 如果同余椭圆曲线的 L 函数在 1 处的取值非零, 则它的秩一定为零. 而且 BSD 猜想断言这是一个充要条件, 因此寻找非同余数的方法应当从 Waldspurger 公式等关于 L 函数特殊值的公式着手. 而田野等人得到的精确 Waldspurger 公式使得 L 函数的特殊值的计算变得可操作.

由于一般的 BSD 猜想并没有被证明, 因此我们无法通过 L 函数特殊值为零得到同余数. 而 Heegner 的方法则告诉我们在椭圆曲线上构造点是可行的, 而且根据 Gross–Zagier 公式点的性质是可以刻画的. 因此寻找同余数就不得不在椭圆曲线上构造 Heegner 点和 Euler 系, 这在 [Tia] 中得以体现.

Heegner 的方法构造出的椭圆曲线的秩为 1, 对于更高的秩, 我们暂时还没有方法构造.

5.2　二次扭系列

同余椭圆曲线是一个特殊的二次扭系列. 对于一般的椭圆曲线我们也可以谈论它们的二次扭系列. 特别地, Coates 等人在这方面对 Birch 引理进行了推广并由此给出了几个带复乘椭圆曲线的秩一二次扭系列. 而我们的第四章给出的正是这种方法在函数域的类比.

5.3　更一般的表示

二次扭的 L 函数可以看成椭圆曲线对应的表示与一个 Dirichlet 特征做张量得到的表示的 L 函数. 更一般地, 我们可以将椭圆曲线与更一般的 Artin 表示做

张量, Darmon, Loffler 和 Zerbes 在这方面做出了较多的工作. 要研究一般的这种问题, 秩零的情形我们需要构造非零的 Euler 系, 利用精确互反律得到上同调类与 p 进 L 函数的联系得到 BSD 猜想. 对于秩一的情形, 我们仍然需要通过构造 Heegner 点来处理.

参考文献

[Art] Arthaud N. **On Birch and Swinnerton-Dyer's conjecture for elliptic curves with complex multiplication I**. Compositio Mathematica, 1978, 37(2): 209–232.

[Boc] Böckle G. **An Eichler-Shimura isomorphism over function fields between Drinfeld modular forms and cohomology classes of crystals**. unpublished.

[BCDT] Breuil C, Conrad B, Diamond F, Taylor R. **On the modularity of elliptic curves over $\mathbb{Q}$: wild 3-adic exercises**. Journal of the American Mathematical Society, 2001, 843–939.

[Bro] Brown M L. **Heegner modules and elliptic curves**. Lecture notes in Mathematics 1849, Springer, 2004.

[BSD] Birch B J, Swinnerton-Dyer H P F. **Notes on elliptic curves II**. J Reine Angew Math, 1965, 218: 79–108.

[Cas] Cassels J W S. **Arithmetic on curves of genus 1, (IV) proof of the Hauptvermutung**. J Reine Angrew Math, 1962, 211:95–112.

[CLTZ] Coates J, Li Y, Tian Y, Zhai S. **Quadratic twists of elliptic curves**. to appear, Proc London Math Soc. Also available at arXiv:1312.3884.

[CoW] Coates J, Wiles A. **On the conjecture of Birch and Swinnerton-Dyer**. Inventiones mathematicae, 1977, 39(3): 223–251.

[Dic] Dickson L E. **History of the theory of numbers**. Vol II, Chelsea Publ Co, New York, 1971.

[Fal] Faltings G. **Endlichkeitssätze für abelsche Varietäten über Zahlkörpern**. Inventiones mathematicae, 1983, 73(3): 349–366.

[冯] 冯克勤. **非同余数和秩零椭圆曲线**. 中国科学技术大学出版社, 2008.

[Fen] Feng K. **Non-congruent numbers, odd graphs and the Birch-Swinnerton-Dyer conjecture**. Acta Arithmetica, 1996, 75: 71–83.

[Gek] Gekeler E U. **Drinfeld Modular Curves**. Lecture Notes in Mathematics 1231, Springer-Verlag, Berlin/New York, 1986.

[GeR] Gekeler E U, Reversat M. **Jacobians of Drinfeld modular curves**. J Reine Angrew Math, 1996, 476: 27–94.

[GrZ] Gross B H, Zagier D B. **Heegner points and derivatives of L-series**. Inventiones mathematicae, 1986, 84(2): 225–320.

[Hay] Hayes D R. **Explicit class field theory in global function fields**. in: Studies in Algebra and Number Theory, in: Adv. in Math. Suppl. Stud., Academic Press, New York, London, 1979, 6: 173–217.

[Har] Hartshorne R. **Algebraic Geometry**. Springer, 1977.

[HeB] Heath-Brown D R. **The size of Selmer groups for the congruent number problem II**. with an appendix by Monsky, Inventiones mathematicae, 1994, 118(1): 331–370.

[Hee] Heegner K. **Diophantische analysis und modulfunktionen**. Math Z, 1952, 56: 227-–253.

[Kna] Knapp A W. **Elliptic Curves**. Princeton University Press, 1993.

[Kob] Koblitz N I. **Introduction to elliptic curves and modular forms**. Springer, 2012.

[Kol] Kolyvagin V A. **Finiteness of $E(\mathbb{Q})$ and $X(E,\mathbb{Q})$ for a class of Weil curves**. Mathematics of the USSR-Izvestiya, 1989, 32(3): 523–541.

[LiT] Li D, Tian Y. **On the Birch-Swinnerton-Dyer conjecture of elliptic curves $E_D : y^2 = x^3 - D^2x$**. Acta Mathematica Sinica ,2000, 16(2): 229–236.

[OuZ] Ouyang Y, Zhang S. **On non-congruent numbers with 1 modulo 4 prime factors**. Sci China Math, 2014, 57(3): 649–658.

[OuZ2] Ouyang Y, Zhang S. **On second 2-descent and non-congruent numbers**. Acta Arithmetica, 2015, 170: 343–360.

[OuZ3] Ouyang Y, Zhang S. **Birch's lemma over global function fields**, submitted.

[Pap] Papikian M. **On the degree of modular parametrizations over function fields**. Journal of number theory, 2002, 97: 317–349.

[Rub] Rubin K. **Elliptic curves with complex multiplication and the conjecture of Birch and Swinnerton-Dyer**. Arithmetic theory of elliptic curves. Springer Berlin Heidelberg, 1999, 167–234.

[Rub2] Rubin K. **The "main conjectures" of Iwasawa theory for imaginary quadratic fields**. Inventiones Mathematicae, 1991, 103(1): 25-–68.

[Sch] Schweizer A. **Hyperelliptic Drinfeld Modular Curves**, in: E.-U Gekeler, M. van der Put, M. Reversat and I. Van Geel (Eds.). Drinfeld Modules, Modular Schemes and Applications, World Sci. Publ., River Edge, NJ, 1997, 330-–343.

[Ser] Serre J P. **A course in arithmetic**. Springer, 2012.

[Sil] Silverman J H. **The Arithmetic of Elliptic Curves**. Graduate Texts in Mathematics, 106, Springer, Dordrecht, 2009.

[Tia] Tian Y. **Congruent numbers and Heegner points**. Camb J Math 2014, 2(1): 117-–161.

[Vig] Vigni S. **On ring class eigenspaces of Mordell–Weil groups of elliptic curves over global function fields**. Journal of Number Theory, 2008, 128: 2159-–2184.

[王] 王章杰. **Cassels 配对和同余曲线**. 中国科学院博士论文.

[WeY] Wei F T, Yu J. **On the independence of Heegner points in the function field case**. Journal of Number Theory, 2010, 130(11): 2542–2560.

[Wil] Wiles A. **Modular elliptic curves and Fermat's last theorem**. Annals of Mathematics, 1995: 443–551.

[XiZ] Xiong M, Zaharescu A. **Selmer groups and Tate-Shararevich groups for the congruent number problem**. Comment Math Helv, 2009, 84(1): 21–56.

致　谢

在中国科学技术大学硕博连读的五年多里，我所从事的学习和研究工作，全部都是在导师以及其他老师和同学的指导和帮助下进行的。在论文完成之际，请容许我对他们表达诚挚的谢意。

首先，感谢导师欧阳毅教授对我多年的细心指导和谆谆教诲。欧阳老师的辛勤指导，让我系统地学习了数论的相关知识。欧阳老师严谨的学术作风、乐观积极的人生态度以及忘我的工作精神，在各个方面影响和感染着我。这些都将成为我人生中宝贵的财富，使我受益终身。

感谢田野教授多年来对我的指导和帮助，让我了解到一个认真、刻苦、努力、优秀的数学工作者该有的工作态度。

感谢王崧、袁新意、张哲、丁一文、杨金榜、熊玮、蔡立、王章结、舒杰、李永雄、刘余、陈轶骅、任远等人给予我的帮助，与你们的讨论使我受益匪浅。

感谢白晓、林秉文、邱国寰、周盾、王皓、蔡延安等同学陪伴我度过的这段愉快而难忘的岁月。

感谢科大，感谢一路走过来的兄弟姐妹们，在这最宝贵的年华中，伴随着我成长。

最后，感谢我的家人，你们一直以来的鼓励与支持是我追求学业的坚强后盾。感谢我的未婚妻王婷婷，你对我的支持永远是我前进的动力。

张神星

二〇一五年九月于合肥

在读期间发表的学术论文与取得的研究成果

[1] Ouyang Y, Zhang S†. **On non-congruent numbers with 1 modulo 4 prime factors**. Sci China Math, 2014, 57(3): 649–658.

[2] Ouyang Y, Zhang S†. **On second 2-descent and non-congruent numbers**. Acta Arithmetica, 2015, 170: 343–360.

[3] Ouyang Y, Zhang S†. **Birch's lemma over global function fields**, 已提交.

[4] Ouyang Y, Zhang S†. **Newton polygons of L-functions of polynomials** $x^d + ax^{d-1}$ **with** $p \equiv -1 \bmod d$, 已提交.

†通讯作者