中国科学技术大学

博士学位论文

同源图及其在密码学上的应用

作者姓名： 徐铮

学科专业： 基础数学

导师姓名： 欧阳毅教授

完成时间： 二〇二四年五月二十八日

University of Science and Technology of China

A dissertation for doctor's degree

Isogeny Graph And Its Application In Cryptography

Author: Xu Zheng

Speciality: Pure Mathematics

Supervisor: Prof. Ouyang Yi

Finished time: May 28, 2024

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

本文研究超奇异椭圆曲线同源图和阿贝尔簇同源图的的结构问题, 决定其中一些顶点的环路和邻域结构.

第一章, 我们介绍超奇异椭圆曲线同源图的研究背景及现有的成果, 给出论文的主要结果; 介绍阿贝尔簇同源图问题相关研究, 给出我们的相关结果.

第二章, 我们给出椭圆曲线的定义和性质, 特别地给出正常和超奇异椭圆曲线的定义和判定条件. 第三章, 我们介绍代数几何的一些基础知识, 包括代数曲线, 代数曲面和阿贝尔簇的基本性质, 并给出超奇异和超特殊阿贝尔簇的定义和性质. 第四章, 我们首先给出超奇异椭圆曲线同源图的定义及其性质, 接下来给出了阿贝尔簇的同源图及其性质. 第五章, 我们介绍超奇异椭圆曲线同源图和阿贝尔簇同源图在密码学中的应用.

第六章, 我们证明论文的主要成果, 即超奇异椭圆曲线同源图上 j-不变量是 0 和 1728 的顶点的环路和邻域结构. 我们的证明方法依据椭圆曲线自同态环的结构和 Deuring 对应定理. 由此, 问题转化为丢番图方程的求解问题以及四元数代数序的左理想类的区分问题. 之后, 我们还给出同源图上 $\mathbb{F}_p$-顶点的环路和邻域相关结果.

第七章, 我们给出超特殊阿贝尔簇同源图上顶点是 $\boldsymbol{E}_{1728} \times \boldsymbol{E}_{1728}$ 和 $\boldsymbol{E}_0 \times \boldsymbol{E}_0$ 的环路结构. 我们的证明方法主要是阿贝尔簇自同态环的结构, 非交换环上的矩阵理论和丢番图分析.

第八章, 我们对同源图研究和它在密码学中的应用作出一些展望.

关键词：有限域上超奇异椭圆曲线；有限域上超特殊阿贝尔簇；自同态环；同源图；理想类；非交换环上的矩阵

ABSTRACT

In this thesis, we study problems related to the structure of the isogeny graphs of supersingular elliptic curves and of abelian varieties, and decide the loops and neighbors of certain vertices.

In Chapter 1, we first review problems and known results about the supersingular elliptic curve isogeny graph and describe the main results of this thesis, then review problems and known results about the abelian varieties graph and describe our results in this subject.

In Chapter 2, we give definitions and properties of elliptic curves, in particular, the definitions and determining criterion of ordinary and supersingular elliptic curves. In Chapter 3, we introduce basic knowledge of algebraic geometry, including algebraic curves, algebraic surfaces and abelian varieties, and also give the definitions and properties of the supersingular and superspecial abelian varieties. In Chapter 4, we introduce the supersingular elliptic curve isogeny graphs and describe their properties, and then introduce the abelian varieties isogeny graphs and study their properties. In Chapter 5, we give an introduction of applications of the supersingular elliptic curve isogeny graph and the abelian varieties isogeny graph in cryptography.

In Chapter 6, we prove our main result about the loops and neighbors of the two vertices whose j-invariants are 0 and 1728 in the supersingular elliptic curve isogeny graph. Our proof is based on the structure of the endomorphism ring and Deuring's correspondence theorem. Our problem is then transformed into solving certain Diophantine equations and distinguishing left ideal classes in a maximal order in certain quaternion algebra. We also describe our result about loops and neighbors of the $\mathbb{F}_p$-vertices in the graph.

In Chapter 7, we determine the number of loops of the vertices $E_{1728} \times E_{1728}$ and $E_0 \times E_0$ on the superspecial abelian varieties isogeny graph. Our proof is based on the study of the structure of endomorphism rings of abelian varieties, theory of matrices over non-commutative rings and Diophantine analysis.

In Chapter 8, we give prospect of isogeny graph and its application in cryptography.

Key Words: Supersingular elliptic curves over finite fields; Superspecial Abelian varieties over finite fields; Endomorphism ring; Isogeny graph; Ideal classes; Matrix over Non-commutative Rings

目　录

第 1 章　内 容 简 介

本章主要介绍论文的研究背景和主要结果以及对之后研究工作的展望.

1.1　椭圆曲线密码学的研究背景

随着量子计算的迅猛发展, 后量子密码学在现代密码学整个学科中的地位日渐上升, 影响力也越来越大. 基于同源的密码体系是后量子密码学的一个重要组成部分, 在美国国家标准技术研究所 (National Institute of Standards and Technology, 简称 NIST) 的后量子密码算法征集计划中, 基于同源的 SIKE 算法进入了第三轮的备选方案.

自 1976 年 Diffie-Hellman 在他们的划时代论文 New Directions in Cryptography 提出公钥密码体系 (Public Key Cryptography, PKC) 以来，公钥密码学已经发展成为全球通信网络的安全基础，对国家和个人信息安全有至关重要的作用. 公钥密码安全通信主要由 Diffie-Hellman 密钥交换、RSA 密码系统和椭圆曲线密码系统来实现，而它们的安全性则取决于大整数分解问题和有限域/椭圆曲线离散对数问题等数论问题的计算困难性. 椭圆曲线在密码学中的应用最早开始于 1986 年, 由 Miller[1] 和 Koblitz[2] 基于椭圆曲线离散对数问题独立提出. 此后椭圆曲线密码 (简称 ECC, 即 Elliptic Curves Cryptography) 成为密码学热门研究方向, 逐渐成为公钥密码的主流, 为保证网络安全起到十分重要的作用. ECC 的安全性基础就是椭圆曲线离散对数问题 (ECDLP), 即对于有限域上椭圆曲线上的两点 P, Q, 如何计算整数 a 使得 $[a]P = Q$. 在经典计算机下, 求解椭圆曲线离散对数的时间复杂度是指数级的[3], 这就保证了 ECC 的安全性.

1994, Peter Shor[4] 提出量子算法, 使得 RSA, ECC 等基于大数分解和离散对数困难问题的公钥密码体系在量子计算机下不再安全. 寻求新的密码体系，抵抗量子攻击，即发展后量子密码体系 (Post-Quantum Cryptography, PQC)，就成为数学界和密码学界的一个关键任务。当前，各国对于 PQC 的研究正如火如荼地开展，期待在未来 5-10 年内有成熟的标准化的抗量子攻击的密码算法，逐渐替代当前通用的公钥密码算法。2016 年 2 月, 美国国家标准技术研究所 (NIST) 启动后量子密码算法标准征集计划，之后欧盟 SAFEcrypto 项目和 PQcrypto 项目. 日本 CREST 项目等也开始了对 PQC 算法标准的研究。2020 年 7 月，NIST 公布了第三轮入选算法作为最终标准化的候选算法，其中包括 4 个公钥加密算法：Class McEliece，CRYSTALS-KYBER，NTRU 和 SABER; 以及 3 个数字签名算法：CRTSTALS-DILITHIUM，FALCON 和 Rainbow。NIST 还公布了 8 个备选算法：

BIKE，FrodoKEM，HQC，NTRU Prime，SIKE，GeMSS，Picnic 和 SPHINCS+，经进一步研究后在将来考虑被标准化. 这些算法按照它们背后的计算困难问题, 可以分为下述四类：基于格，基于多变量，基于编码和基于同源. 本论文研究超奇异椭圆曲线同源图的结构, 是超奇异椭圆曲线同源构造问题研究的一条重要技术路线, 与基于超奇异椭圆曲线同源构造问题的后量子密码体系 (SIKE) 紧密关联.

我们首先介绍一下超奇异椭圆曲线同源图在密码学上的应用. 2006 年, Charles-Lauter-Goren[5] 根据超奇异椭圆曲线同源图的路径寻找问题, 设计哈希函数. 他们首次将椭圆曲线同源用在了哈希函数上, 得到了在后量子密码学里的应用. 2009 年, Rostovtsev-Stolbunov[6] 基于正常椭圆曲线之间的同源计算问题, 设计了一个 Diffie-Hellman 密钥交换协议, 这是椭圆曲线同源的第二个密码学的应用. 2011 年开始, Jao-De Feo[7] 设计了基于超奇异同源 Diffie-Hellman 密钥交换, 称之为 SIDH. 这是椭圆曲线同源的第三个密码学的应用. 2018 年, Castryck-Lange-Martindale-Panny-Renes[8] 设计基于超奇异椭圆曲线同源的非交互的 Diffie-Hellman 密钥交换, 称之为 CSIDH. 这是椭圆曲线同源的第四个密码学应用. 2016 年, NIST 启动后量子密码征集, 基于后量子密码学问题 SIDH 的密码算法 SIKE 被提出并提交到 NIST. 2020 年, SIKE 入选第三轮备选算法.

基于同源的超奇异椭圆曲线后量子密码体系中考虑的主要数学问题包括：同源计算问题, 自同态环的计算问题和同源图的结构问题. 超奇异椭圆曲线同源的计算问题和超奇异椭圆曲线自同态环的计算问题是等价的, 这也是保证哈希函数, SIDH-密钥交换, CSDIH-密钥交换的安全性的关键. 超奇异椭圆曲线同源图结构直接决定了路径寻找, 也就决定了超奇异椭圆曲线同源的计算问题, 因此它在椭圆曲线后量子密码体制中起到重要的作用

我们简述一下同源计算问题研究的系列进展. 2008 年, Charles-Goren-Lauter[5] 提出通过 Pollard-rho 攻击算法计算同源复杂度是 $O(p^{\frac{1}{2}}\log^2 p) = \tilde{O}(p^{\frac{1}{2}})$. 2012 年, Childs-Jao-Soukharev[9] 提出在量子计算机下, 存在亚指数时间的算法正常椭圆曲线之间的同源, 这就说明 Rostovtsev-Stolbunov 的密钥交换协议不能抵抗量子攻击. 2014 年, Biasse-Jao-Sankar[10], 将定义在 $\mathbb{F}_{p^2}$ 上的超奇异椭圆曲线通过量子 Grover 算法找到像是定义在 $\mathbb{F}_p$ 上的超奇异椭圆曲线的同源, 算法的时间复杂度是 $\tilde{O}(p^{\frac{1}{4}})$, 再利用量子算法得到 $\mathbb{F}_p$ 上的同源, 时间复杂度是 $L_p(\frac{1}{2}, \frac{\sqrt{3}}{2})$, 由此可以计算同源时间复杂度是 $\tilde{O}(p^{\frac{1}{4}})$. 2014 年, Jao-De Feo[7] 提出超奇异椭圆曲线同源计算在经典计算机下时间复杂度是 $\tilde{O}(p^{\frac{1}{4}})$, 在量子计算机下时间复杂度是 $\tilde{O}(p^{\frac{1}{6}})$. 2016 年, Delfs-Galbraith[11] 提出了计算定义在 $\mathbb{F}_p$ 上超奇异椭圆曲线同源的算法, 计算复杂度是 $\tilde{O}(p^{\frac{1}{4}})$, 在一般域上计算复杂度仍为 $\tilde{O}(p^{\frac{1}{2}})$. 2020 年, Love-Boneh[12] 对于自同态环中含有特定元素的超奇异椭圆曲线给出计算其同源的多项式时间的概率算法.

同源计算与自同态环的关系主要有下述研究. 2014 年, Kohel-Lauter-Petit-Tignol[13] 提出在已知超奇异椭圆曲线自同态环情况下, 通过强逼近定理计算四元数代数极大序的约化范数是 ℓ 的方幂的左理想的多项式时间概率算法, 来得到超奇异椭圆曲线之间的同源. 这样将 SIDH 中计算同源的问题约化到了计算自同态环上. 2020 年, Castryc-Panny-Vercauteren[14] 对于两条 $\mathbb{F}_p$ 自同态环相同的定义在 $\mathbb{F}_p$ 上的超奇异椭圆曲线提出多项式时间算法去计算连接它们之间的理想, 找到相应的同源. 这样将 CSIDH 中计算同源的问题约化到了计算超奇异椭圆曲线自同态环.

关于自同态环的计算, 则主要有下述系列研究. 1996 年, Kohel[15] 在博士论文中首先提出了计算超奇异椭圆曲线自同态环, 论文给出计算出四个线性无关的圈的算法, 由此给出自同态环的子序. 确定性算法时间复杂度是 $O(p^{\frac{3}{2}+\epsilon})$, 概率算法时间复杂度是 $O(p^{1+\epsilon})$. 2004 年, Cervino[16] 对于定义在 $\mathbb{F}_p$ 上的超奇异椭圆曲线计算自同态环的算法时间复杂度是 $\tilde{O}(p^{2.5})$, 对于一般的超奇异椭圆曲线计算自同态环的算法时间复杂度是 $\tilde{O}(p^4)$. 2011 年, Bisson-Sutherland[17] 给出计算正常椭圆曲线自同态环的亚指数时间算法. 2014 年, Chevyrev-Galbraith[18] 提升了 Cervino 的算法, 将 $\tilde{O}(p^{2.5})$ 提升为 $O(p^{1+\epsilon})$, 将 $\tilde{O}(p^4)$ 提升为 $O(p^{2.5+\epsilon})$. 2019 年, Bank–Navarro-Eisentrager-Morrison -Park[19] 继续研究了 Kohel 的问题, 并给出两个圈不能生成自同态环的条件. 2020 年, Eisenträger-Hallgren-Leonardi-Morrison-Park[20] 通过找到超奇异椭圆曲线中的两个自同态来生成自同态环, 其计算复杂度是 $O(p^{\frac{1}{2}}\log^2 p) = \tilde{O}(p^{\frac{1}{2}})$. 这一结果也攻击了哈希函数中的第二原像寻找问题.

同源图的结构是我们论文研究的主要问题, 目前主要有下面这些结果. 2008 年, Charles-Goren-Lauter[5] 首次提出了 CGL 哈希函数的路径寻找, 密码学家便将关注点集中在超奇异椭圆曲线同源图问题上. 2016 年, Delfs-Galbraith[11] 对于定义在 $\mathbb{F}_p$ 上的超奇异椭圆曲线同源图进行了研究, 给出了同源图的上升下降水平的同源个数, 由此可以得到超奇异椭圆曲线的 $\mathbb{F}_p$ 同源图的结构. 2019 年, Adj[21] 研究了对于不同的迹, 即 $\mathrm{tr}(\pi) = 0, \pm p$ 时, 关于图 $\mathcal{G}_\ell(\overline{\mathbb{F}}_p)$ 上的结构, 并给出了对于 $\mathrm{tr}(\pi) = \pm 2p$, $p > 4\ell$ 时, $j = 1728$ 在同源图中环路的个数. 2019 年, 欧阳毅和本文作者[22] 给出 $j = 0$ 时对应的环路的个数. 2020 年, 李宋宋, 欧阳毅和本文作者[23][24] 给出 $j = 0$ 和 1728 时对应的邻域结构以及定义在 $\mathbb{F}_p$ 上同源的个数, 并给出了 j-不变量落到 $\mathbb{F}_p$ 上时相应的结果. 2018 年, Eisentrager-Hallgren-Lauter-Morrison-Petit[25] 将以上问题做了约化, 指出了计算超奇异椭圆曲线之间的同源问题和计算超奇异椭圆曲线自同态环之间是等价的, 当然这些问题也和 CGL 哈希函数中的第一原像寻找和碰撞问题是等价的.

1.2　超奇异椭圆曲线同源图的主要结果

本论文主要研究超奇异椭圆曲线同源图的结构问题, 主要是同源图的顶点之间的连接关系. 论文首次将丢番图分析方法引入到同源图的计算中, 得到椭圆曲线 $\overline{\mathbb{F}_p}$-同源图结构一些结果, 开创了同源图研究新的方向, 这对于计算超奇异椭圆曲线同源和路径寻找提供了有效的帮助, 有助于解决现有的后量子密码学问题: CGL-哈希函数, SIDH 密钥交换和 CSIDH 密钥交换. 总的来说, 我们的工作推进了同源图结构研究和具体计算, 并很好地应用到具体实践中. 在我们的结果发表以后, Onuki-Aikawa-Takagi[26] 也采用我们的丢番图分析方法到具体的 SIKE 计算中, 并对于 SIKEp434 和 SIKEp503 上的同源计算和路径寻找做了具体的分析, 给出了具体的算法.

设 p 和 ℓ 是素数, 本论文研究定义在 $\overline{\mathbb{F}}_p$ 上超奇异椭圆曲线 ℓ-同源图的结构. 注意到此时可以将椭圆曲线和它的 j-不变量等同起来. 设 π 是 E 的 $\mathbb{F}_p$-Frobenius, $\mathrm{tr}(\pi) = \mathrm{tr}(E)$ 是它的迹.

Adj 等[21] 给出了当 $\mathrm{tr}(E) = \pm 2p$, $p > 4\ell$ 时, 顶点 $j = 0, 1728$ 在 ℓ-超奇异同源图中环路的个数. 但我们发现对于 $j = 0$, $p > 4\ell$ 并不是环路个数最好的界, 我们给出更好的界 $p > 3\ell$. 具体的计算结果表明我们实际上得到了最优界. 这是我们的第一个成果 [22]. 我们进一步给顶点 $j = 0$ 和 1728 在 ℓ-同源图中的邻域结构以及定义在 $\mathbb{F}_p$ 上同源的个数, 这是我们的第二个结果 [23]. 最后我们给出了 j-不变量落到 $\mathbb{F}_p$ 上时的邻域的结构. 这是我们的第三个结果 [24]. 我们还通过具体计算获得的数据来表明论文得到的结果都是最优的.

以下具体说明一下李宋宋, 欧阳毅和本文作者 [22] [23] [24] 得到的结果.

记超奇异椭圆曲线 E 的自同态环 $\mathrm{End}(E) = \mathcal{O}$, 由 [27], [28], 我们有：

- 当 $j = 1728$ 时,

$$\mathcal{O} = \mathrm{End}(E_{1728}) = \mathbb{Z} + \mathbb{Z}i + \mathbb{Z}\frac{1+j}{2} + \mathbb{Z}\frac{i+k}{2},$$

  其中 $i^2 = -1$, $j^2 = -p$, $ij = -ji = k$.

- 当 $j = 0$ 时,

$$\mathcal{O} = \mathrm{End}(E_0) = \mathbb{Z} + \mathbb{Z}\frac{1+i}{2} + \mathbb{Z}\frac{i+k}{3} + \mathbb{Z}\frac{j+k}{2},$$

  其中 $i^2 = -3$, $j^2 = -p$, $ij = -ji = k$.

- $j \in \mathbb{F}_p \backslash \{0, 1728\}$ 时, 若 $\frac{1+\pi}{2} \notin \mathrm{End}(E)$,

$$\mathcal{O} = \mathrm{End}(E) = \mathbb{Z} + \mathbb{Z}\frac{1+i}{2} + \mathbb{Z}\frac{j-k}{2} + \mathbb{Z}\frac{ri-k}{q},$$

  其中 $(\frac{p}{q}) = -1$, $q \equiv 3 \bmod 8$, $r^2 \equiv -p \bmod q$, $i^2 = -q$, $j^2 = -p$, $ij = -ji = k$.

- $j \in \mathbb{F}_p \backslash \{0, 1728\}$ 时, 若 $\frac{1+\pi}{2} \in \mathrm{End}(E)$，

$$\mathcal{O} = \mathrm{End}(E) = \mathbb{Z} + \mathbb{Z}\frac{1+j}{2} + \mathbb{Z}i + \mathbb{Z}\frac{r'i - k}{2q},$$

其中 $(\frac{p}{q}) = -1$, $q \equiv 3 \bmod 8$, $r'^2 \equiv -p \bmod 4q$, $i^2 = -q$, $j^2 = -p$, $ij = -ji = k$.

对于负整数 D，令

$$\delta_D = \begin{cases} 1, & \text{若 } (\frac{D}{\ell}) = 1 \text{ 且 Hilbert 类多项式 } H_D(x) \text{ 在 } \mathbb{F}_\ell \text{ 分裂;} \\ -1, & \text{其他情况.} \end{cases} \tag{1.1}$$

有了这些准备, 我们可以叙述论文的主要结果. 关于超奇异椭圆曲线 ℓ-同源图 $\mathcal{G}_\ell(\overline{\mathbb{F}}_p)$ 上顶点的环路, 我们得到

定理 1.1　考虑超奇异椭圆曲线 ℓ-同源图 $\mathcal{G}_\ell(\overline{\mathbb{F}}_p)$.

(1) 对于 $j = 1728$ 的超奇异椭圆曲线 E_{1728} (此时 $p \equiv 3 \bmod 4$), 当 $p > 4\ell$ 时,
   (i) 当 $\ell \equiv 1 \bmod 4$ 时, 顶点 $[E_{1728}]$ 有两条环路;
   (ii) 当 $\ell \equiv 3 \bmod 4$ 时, 顶点 $[E_{1728}]$ 没有环路;
   (iii) 当 $\ell = 2$ 时, 顶点 $[E_{1728}]$ 有一条环路.

(2) 对于 $j = 0$ 的超奇异椭圆曲线 E_0 (此时 $p \equiv 2 \bmod 3$), 当 $p > 3\ell$ 时,
   (i) 当 $\ell \equiv 1 \bmod 3$ 时, 顶点 $[E_0]$ 有两条环路;
   (ii) 当 $\ell \equiv 2 \bmod 3$ 时, 顶点 $[E_0]$ 没有环路;
   (iii) 当 $\ell = 2$ 时, 顶点 $[E_0]$ 没有环路;
   (iv) 当 $\ell = 3$ 时, 顶点 $[E_0]$ 有一条环路.

(3) 设 E 是超奇异椭圆曲线 E, $j(E) \in \mathbb{F}_p$ 但 $j \neq 0, 1728$.
   (i) 若 $\frac{1+\pi}{2} \notin \mathcal{O}$, 当 $p > q\ell$ 时, 顶点 $[E]$ 处有 $1 + \delta_{-q}$ 条环路;
   (ii) 若 $\frac{1+\pi}{2} \in \mathcal{O}$, 当 $p > 4q\ell$ 时, 顶点 $[E]$ 处有 $1 + \delta_{-4q}$ 条环路.

关于顶点的邻域结构, 则有如下结果:

定理 1.2　考虑超奇异椭圆曲线 ℓ-同源图 $\mathcal{G}_\ell(\overline{\mathbb{F}}_p)$.

(1) 设 $\ell > 3$. 若 $p \equiv 3 \bmod 4$ 且 $p > 4\ell^2$, 则 $[E_{1728}]$ 在图中存在 $\frac{1}{2}\left(\ell - (-1)^{\frac{\ell-1}{2}}\right)$ 个邻接, 且通过两条边连接每个邻接.

(2) 设 $\ell > 3$. 若 $p \equiv 2 \bmod 3$ 且 $p > 3\ell^2$, 则 $[E_0]$ 在图中存在 $\frac{1}{3}(\ell - (\frac{\ell}{3}))$ 个邻接, 通过三条边连接连接每个邻接.

(3) 设 E 是超奇异椭圆曲线 E, $j(E) \in \mathbb{F}_p$ 但 $j \neq 0, 1728$.
   (i) 若 $\frac{1+\pi}{2} \notin \mathcal{O}$, 当 $p > q\ell^2$ 时, $[E]$ 通过一重边连接到 $\ell - \delta_{-q}$ 个不同的椭圆曲线;
   (ii) 若 $\frac{1+\pi}{2} \in \mathcal{O}$, 当 $p > 4q\ell^2$ 时, $[E]$ 通过一重边连接到 $\ell - \delta_{-4q}$ 个不同的椭圆曲线.

关于 $\mathbb{F}_p$ 同源个数的, 则有下面的结果:

定理 1.3　考虑超奇异椭圆曲线 ℓ-同源图 $\mathcal{G}_\ell(\overline{\mathbb{F}}_p)$.

(1) 对于 $j=1728$, 当 $p>4\ell^2$ 时, 有 $1+(\frac{\ell}{p})$ 个与 $[E_{1728}]$ 相连的顶点的 j-不变量落在 $\mathbb{F}_p-\{1728\}$ 中.

(2) 对于 $j=0$, 当 $p>3\ell^2$ 时, 有 $1+(\frac{-p}{\ell})$ 个与 $[E_0]$ 相连的顶点的 j-不变量落在 $\mathbb{F}_p^*$ 中.

(3) 设 E 是超奇异椭圆曲线 E, $j(E)\in\mathbb{F}_p$ 但 $j\neq 0,1728$.

(i) $\frac{1+\pi}{2}\notin\mathcal{O}$ 时, 若 $p>q\ell^2$, 则有 $1+(\frac{-p}{\ell})$ 个邻域在 $\mathbb{F}_p$ 上;

(ii) $\frac{1+\pi}{2}\in\mathcal{O}$ 时, 若 $p>4q\ell^2$, 则有 $1+(\frac{-p}{\ell})$ 个邻域在 $\mathbb{F}_p$ 上.

我们将在第二章中介绍椭圆曲线的基础知识, 复数域上椭圆曲线的复乘, 有限域上椭圆曲线的分类：正常椭圆曲线和超奇异椭圆曲线, 并给出四元数代数的算术性质以及 Deuring 对应. 在第四章中给出有限域上椭圆曲线同源图及其性质, 包括：$\mathbb{F}_p$-图, $\mathbb{F}_{p^2}$-图和 $\overline{\mathbb{F}}_p$-图. 在第六章我们给出上述定理的证明.

1.3　超奇异阿贝尔簇密码学的研究背景

2018 年以后, 随着椭圆曲线在后量子密码学的应用的深入, 数学家和密码学家尝试将更多的算术几何工具应用到密码学上, 这促成了对于维数 2 的阿贝尔簇上的同源计算问题的研究, 基于超特殊阿贝尔簇的 Richelot 同源图的哈希函数构造和超奇异阿贝尔簇的 Diffie-Hellman 密钥交换协议等.

具体说来, 最近几年特别是近三年来超奇异阿贝尔簇的同源计算问题和它的密码学应用受到广泛关注.

2014 年, Inoica-Thome[29] 首先提出了带极大实乘的正常阿贝尔簇同源图, 在类数是 1 的全实子域上做理想的分解, 根据理想的作用定义和椭圆曲线类似的上升水平和下降, 并通过配对给出同源是上升水平和下降的充要条件, 由此定义带极大实乘的正常阿贝尔簇同源图.

2019 年, Springer[30] 给出计算带极大实乘的正常阿贝尔簇的自同态环的算法, 计算复杂度是亚指数时间复杂度. 同样在 2019 年, Flynn-Ti[31] 提出了基于二维主极化阿贝尔簇的同源的密钥交换协议，称之为亏格 2 的 SIDH. 他们将原先的 SIDH 中的 ℓ-同源变成了超椭圆曲线的雅可比簇上的 (ℓ,ℓ)-同源, 从而得到类似的密钥交换协议. 他们还具体计算了主极化超奇异阿贝尔簇的同源和 (ℓ,ℓ) 同源的个数.

2020 年, Castryck-Decru-Smith[32] 提出了超特殊 Richelot 同源图的定义, 给出 15 个 Richelot 同源的构造和计算, 并给出同源图顶点的个数, 同源图中输出边的个数, 以及输入边的界, 提出了基于超特殊阿贝尔簇的 Richelot 同源图的哈希函数构造. 他们将原先的哈希函数中的椭圆曲线和 2-同源换成了超椭圆曲线的雅

可比簇和 $(2,2)$-同源, 把原先的 1 比特变成了 3 比特. Katsura-Takashima[33] 利用约化的自同构群给出了更好的关于超特殊同源图的刻画和结果, 得到从雅可比簇出来的到椭圆曲线乘积的同源个数是约化自同构群里长二阶元的个数, 并由此对 Richelot 同源图进行分类. Jordan-Zaytman[34] 给出了用矩阵描述主极化除子以及同源, 并得到了它们的对应关系, 由此利用强逼近定理证明了超特殊阿贝尔簇同源图是连通图. Costello-Smith[35] 给出计算 g 维超特殊主极化阿贝尔簇之间的 $(\ell)^g$ 同源的算法, 在经典计算机下概率算法时间复杂度是 $\tilde{O}(p^{g-1})$, 在量子计算机下算法时间复杂度是 $\tilde{O}(\sqrt{p^{g-1}})$.

2021 年, Florit-Smith[36][37] 通过约化自同构群作用在极大 2-韦伊迷向子群上划分轨道和稳定化子并具体计算得到部分的 Richelot 同源图. 同年 Katsura[38] 研究了亏格是 3 的超椭圆曲线的雅可比簇的 $(2,2,2)$ 同源, 将原先的结果推广到三维上.

2021 年, 欧阳毅和本文作者[39] 给出 $E_{1728}\times E_{1728}$ 和 $E_0\times E_0$ 对应的环路的个数.

当前, 阿贝尔簇上的同源计算研究中有两个方面的问题需要着重考虑：

(1) 在用约化自同构群去划分 Richelot 同源图时, 图中是否存在不同形式的边仍连到同一个顶点? 约化自同构群只是把图做了第一步分类, 但之后的分类, 可能和在椭圆曲线同源图计算出现的情形一样, 也依赖于 p 和 ℓ 的关系.

(2) 如何用矩阵来描述同源关系? 现在, 人们已经可以通过计算非交换环上的矩阵来计算对应的同源, 具体计算正是之后研究工作需要努力的方向. 另外, 人们仍不清楚不同的主极化除子对应的矩阵以及非交换环上的矩阵计算相关问题.

1.4　超特殊阿贝尔簇同源图的主要结果

我们主要研究的是超特殊主极化阿贝尔簇同源图的结构, 引入了非交换环上的矩阵的计算方法, 通过丢番图分析计算同源. 这与之前只通过约化自同构群计算同源不同. 由于一般的结果需要 p 和 ℓ 之间的关系, 所以只通过约化自同构群计算出来的结果只有第一步的分类, 即分类是不完全的, 不具有一般性. 而我们得到的是一般性的结果, 对于同源次数的要求也具有一般性. 这个结果开创了对超特殊主极化阿贝尔簇 (ℓ,ℓ) 同源图的具体研究, 这对之后将 $(2,2)$-同源推广到 (ℓ,ℓ) 同源会有很大的启发意义.

这项工作对计算超奇异椭圆曲线同源和路径寻找将提供有效的帮助, 有助于解决现有的后量子密码学问题: 超特殊阿贝尔簇的哈希函数, 亏格 2 的 SIDH 密钥交换协议. 阿贝尔簇后量子密码学研究最近才兴起, 我们也是最早开始研究阿

贝尔簇同源图计算的, 这对之后的研究将指出具体方向.

以下具体说明一下欧阳毅和本文作者 [39] 得到的结果.

我们的主要结果是同源图上给出特殊的两个顶点 $\boldsymbol{E}_{1728}\times\boldsymbol{E}_{1728}$ 和 $\boldsymbol{E}_0\times\boldsymbol{E}_0$ 上的环路的个数：

定理 1.4 [39]

(1) 对于超特殊阿贝尔簇 $\boldsymbol{E}_{1728}\times\boldsymbol{E}_{1728}$(此时 $p\equiv 3 \bmod 4$), 当 $p>4\ell$ 时, 在阿贝尔簇 (ℓ,ℓ)-同源图中有:

(i) 当 $\ell\equiv 1 \bmod 4$ 时, $\boldsymbol{E}_{1728}\times\boldsymbol{E}_{1728}$ 有 $\ell+3$ 条环路;

(ii) 当 $\ell\equiv 3 \bmod 4$ 时, $\boldsymbol{E}_{1728}\times\boldsymbol{E}_{1728}$ 有 $\ell+1$ 条环路;

(iii) 当 $\ell=2$ 时, $\boldsymbol{E}_{1728}\times\boldsymbol{E}_{1728}$ 有三条环路.

(2) 对于超特殊阿贝尔簇 $\boldsymbol{E}_0\times\boldsymbol{E}_0$(此时 $p\equiv 2 \bmod 3$), 当 $p>3\ell$ 时, 在阿贝尔簇 (ℓ,ℓ) 同源图中有:

(i) 当 $\ell\equiv 1 \bmod 3$ 时, $\boldsymbol{E}_0\times\boldsymbol{E}_0$ 有 $\ell+3$ 条环路;

(ii) 当 $\ell\equiv 2 \bmod 3$ 时, $\boldsymbol{E}_0\times\boldsymbol{E}_0$ 有 $\ell+1$ 条环路;

(iii) 当 $\ell=3$ 时, $\boldsymbol{E}_0\times\boldsymbol{E}_0$ 有一条环路.

我们将在第三章中介绍代数几何的基础知识, 包括代数曲线和代数曲面, 复数域上阿贝尔簇的定义, 有限域上阿贝尔簇, 超奇异阿贝尔簇和超特殊阿贝尔簇等. 在第四章中我们给出有限域上阿贝尔簇的同源图及其性质, 包括：超奇异主极化阿贝尔簇同源图, 超特殊主极化阿贝尔簇 Richelot 同源图, 超特殊主极化阿贝尔簇 (ℓ,ℓ)-同源图. 在第七章我们给出上述定理的证明.

第 2 章　椭圆曲线基础知识

本章中我们将给出椭圆曲线的基础知识，包括在不同域上的形式和性质: 复数域，有限域等，以及椭圆曲线同源的定义. 这部分的基础知识可以参考 [40], [41], [42] 和 [43] 等.

2.1　椭圆曲线

2.1.1　椭圆曲线

令 K 为一个域, $\overline{K}$ 为 K 的代数闭包.

定义 2.1　定义在域 K 上的椭圆曲线 E/K 是域上包含一个有理点 O (通常称为无穷远点), 亏格是 1 的非奇异代数曲线.

定义 2.2　设平面曲线 E 是定义在域 K 上且无穷远点 $O = [0, 1, 0]$ 的椭圆曲线. 那么 E 的仿射部分是由三次方程

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \text{ 其中 } a_1, \cdots, a_6 \in K, \tag{2.1}$$

定义的非奇异曲线, 此方程称为 E 的 Weierstrass 方程.

当域 K 的特征不为 2 时, 通过换元 (仿射变换) 可以得到新的 Weierstrass 方程:

$$y^2 = 4x^3 + b_2x^2 + 2b_4x + b_6, \tag{2.2}$$

其中:

$$b_2 = a_1^2 + 4a_2, \quad b_4 = 2a_4 + a_1a_3,$$
$$b_6 = {a_3}^2 + 4a_6, \quad b_8 = a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2.$$

更进一步地, 当域的特征不为 3 时, 通过换元可以得到方程

$$y^2 = x^3 - 27c_4x - 54c_6, \tag{2.3}$$

其中:

$$c_4 = b_2^2 - 24b_4, \quad c_6 = -b_2^3 + 36b_2b_4 - 216b_6.$$

定义 2.3　椭圆曲线 E 的判别式定义为方程 (2.1) 的判别式, 即

$$\triangle = -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6, \tag{2.4}$$

它的 j 不变量定义为

$$j = \frac{c_4^3}{\triangle}. \tag{2.5}$$

记 E 的有理函数域为 $K(E)$.

由于平面曲线非奇异当且仅当对应的曲线方程判别式不等于 0，故椭圆曲线的判别式都不是 0. 对于 j-不变量, 则有:

定理 2.1 (Tate)　定义在域 K 上的两条椭圆曲线在 K 的代数闭包 $\overline{K}$ 中同构当且仅当它们有相同的 j-不变量.

证明　证明参考 [40] 第三章性质 1.4(b). □

2.1.2　除子与椭圆曲线加法

对于一般的诺特整分离概型且余一维是正则的, 素除子是余一维闭整子概型. 而椭圆曲线是一维的, 所以其上的除子素除子是闭点 (点)P 的形式, 我们称之为点除子.

定义 2.4　椭圆曲线 E 上的 Weil 除子的定义为 $D = \sum n_P P$, 其中 P 是 E 上的点, n_P 是整数, 且只有有限个 n_P 不为 0.

Weil 除子 D 的次数 $\deg D = \sum_P n_P$. 若对所有 P 均有 $n_P \geqslant 0$, 则称除子为有效除子.

记椭圆曲线 E 上全体 Weil 除子的集合为 $\mathrm{Div}(E)$, 记其中次数 0 的全体 Weil 除子的集合为 $\mathrm{Div}^0(E)$.

定义 2.5　对于非零有理函数 $f \in K(E)$, 定义 $\mathrm{div}(f) = \sum_P \upsilon_P(f)P$, 称为 f 对应的主除子, 它的次数 $\deg(\mathrm{div}(f)) = 0$, 记全体主除子的集合是 $\mathrm{Pri}(E)$.

E 的除子类群 $\mathrm{Cl}(E) = \mathrm{Div}(E)/\mathrm{Pri}(E)$, 雅可比 $\mathrm{Jac}(E) = \mathrm{Pic}^0(E) = \mathrm{Div}^0(E)/\mathrm{Pri}(E)$.

定理 2.2　对于椭圆曲线 E, 我们有 E 的 $\overline{K}$ 有理点和 $\mathrm{Pic}^0(E)$ 有一一对应：

$$\theta : E(\overline{K}) \to \mathrm{Pic}^0(E); \qquad P \to [P - O].$$

证明　证明参考 [40] 第三章性质 3.4. □

由此, 可以通过有理点和雅可比的对应关系来定义椭圆曲线的加法.

2.2　同源

定义 2.6　若 $\phi : E_1 \to E_2$ 是椭圆曲线间的态射且 $\phi(O) = O$, 则称 ϕ 是椭圆曲线的同源.

同源有两种情况：

(1) $\phi(E_1) = O$, 此时称为零同源.

(2) $\phi(E_1) = E_2$, 此时 $K(E_1)$ 是 $K(E_2)$ 的有限扩张, 且 ϕ 是有限加法满同态, 故 $\ker(\phi)$ 是有限子群.

非常值同源 ϕ 诱导域的嵌入

$$\phi^* : \overline{K}(E_2) \to \overline{K}(E_1),\ f \to f \circ \phi.$$

定义 2.7　同源 ϕ 的次数 $\deg(\phi)$ 定义为 $\ker(\phi)$ 的阶, 亦即域扩张次数 $[\overline{K}(E_1) : \phi^*\overline{K}(E_2)]$. 零同源的次数定义为 0.

命题 2.3　存在唯一的同源 $\hat{\phi} : E_2 \to E_1$, 使得 $\phi \circ \hat{\phi} = [\deg(\phi)]$, $\hat{\phi} \circ \phi = [\deg(\phi)]$. 这里 $[m]$ 表示倍乘运算. 此时称 $\hat{\phi}$ 为 ϕ 的对偶.

证明　证明参考 [40] 第三章性质 6.2(a). □

定义 2.8　由 E 到 E 的同源称为自同态. 定义在 $\overline{K}$ 上的自同态全体构成一个环, 称为自同态环, 记为 $\mathrm{End}(E)$.

自同态环中包含了数乘全体, 即包含了 $\mathbb{Z}$. 如果椭圆曲线的自同态环大于 $\mathbb{Z}$, 则称该椭圆曲线带复乘.

自同态环中的可逆元称为自同构. 所有自同构组成的乘法群称为椭圆曲线的自同构群, 记作 $\mathrm{Aut}(E)$.

关于椭圆曲线的自同构群, 有下面结果:

命题 2.4　对于域 K 上的椭圆曲线 E, 当 $\mathrm{char}(K) \neq 2, 3$ 时, 自同构群 $\mathrm{Aut}(E)$ 有以下情况：

(1) 当 $j \neq 0, 1728$ 时, $\mathrm{Aut}(E) = \{1, -1\}$;

(2) 当 $j = 1728$ 时, $\mathrm{Aut}(E) = \{1, -1, \alpha, -\alpha\}$, 其中 $\alpha : (x, y) \to (-x, yi)$, $i^2 = -1$;

(3) 当 $j = 0$ 时, $\mathrm{Aut}(E) = \{1, -1, \beta, -\beta, \beta^2, -\beta^2\}$, 其中 $\beta : (x, y) \to (\omega x, -y)$, ω 为三次单位根.

证明　证明参考 [40] 第三章定理 10.1. □

2.3　复数域上的椭圆曲线

2.3.1　复环面和椭圆曲线的对应

定义 2.9　复数域上的环面即 $\mathbb{C}/\Lambda$, 其中 $\Lambda = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$ 为一个格, ω_1, ω_2 是 $\mathbb{R}$-线性无关的.

两个格 Λ_1, Λ_2 称为是位似的, 若存在 $\alpha \in \mathbb{C}^\times$, 使得 $\Lambda_1 = \alpha\Lambda_2$.

定义 2.10　设 Λ 是 $\mathbb{C}$ 上的格. 椭圆曲线 $E_\Lambda/\mathbb{C}$ 即

$$E_\Lambda : y^2 = 4x^3 - g_2(\Lambda)x - g_3(\Lambda) \tag{2.6}$$

其中

$$g_2(\Lambda) = 60G_4(\Lambda) = 60\sum_{\omega\in\Lambda}\frac{1}{\omega^4},$$
$$g_3(\Lambda) = 140G_6(\Lambda) = 140\sum_{\omega\in\Lambda}\frac{1}{\omega^6}.$$

椭圆曲线 E_Λ 和复环面 $\mathbb{C}/\Lambda$ 有对应关系:

定理 2.5　如下映射 Φ 给出椭圆曲线 E_Λ 和复环面 $\mathbb{C}/\Lambda$ 间的同构:

$$\Phi : \mathbb{C}/\Lambda \to E_\Lambda(\mathbb{C});$$
$$z \to \begin{cases} (\wp(z), \wp'(z)), & z \notin \Lambda \\ O, & z \in \Lambda \end{cases}$$

其中

$$\wp(z) = \frac{1}{z^2} + \sum_{\omega\in\Lambda,\omega\neq 0}\left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2}\right)$$

为 Weierstrass $\wp$-函数. 此时, 椭圆曲线 E_Λ 的 j 不变量为 $1728\frac{g_2(\Lambda)^2}{g_2(\Lambda)-27g_3(\Lambda)}$.

证明　参考 [40] 第六章性质 3.6. □

命题 2.6　若格 Λ_1, Λ_2 是位似的, 则 $j(E_{\Lambda_1}) = j(E_{\Lambda_2})$.

证明　参考 [43] 定理 10. 9. □

2.3.2　复数域上椭圆曲线的同源

设 Λ_1, Λ_2 为两个格. 若 $\alpha\Lambda_1 \subseteq \Lambda_2$, 则

$$\phi_\alpha : \mathbb{C}/\Lambda_1 \to \mathbb{C}/\Lambda_2,\ z + \Lambda_1 \to \alpha z + \Lambda_2$$

是全纯映射, 通过同构 Φ 给出了椭圆曲线间的一个同源. 从而有:

定理 2.7　设 Λ_1, Λ_2 为 $\mathbb{C}$ 中的两个格, 对应椭圆曲线 E_1, E_2. 则

$$\begin{aligned}\{\text{同源} : E_1 \to E_2\} &\leftrightarrow \{\alpha \in \mathbb{C} \mid \alpha\Lambda_1 \subseteq \Lambda_2\} \\ &\leftrightarrow \{\text{全纯映射}\phi : \mathbb{C}/\Lambda_1 \to \mathbb{C}/\Lambda_2, \phi(0) = 0\}\end{aligned}$$

三者是一一对应.

证明　参考 [40] 第六章定理 4.1. □

定义 2.11　当 $\Lambda_1 = \Lambda_2 = \Lambda$ 时, 设 $E = E_\Lambda$. 则 $\mathrm{End}(E) \cong \{\alpha \in \mathbb{C} \mid \alpha\Lambda \subseteq \Lambda\}$(这里 α 对应 ϕ_α). 此时定义 $\mathrm{tr}(\alpha) = \alpha + \bar{\alpha}$, $\mathrm{Nr}(\alpha) = \alpha\bar{\alpha}$. 则 $\mathrm{tr}(\alpha) = \mathrm{tr}(\phi_\alpha)$, $\mathrm{Nr}(\alpha) = \deg(\phi_\alpha)$.

2.3.3　模多项式

定义 2.12　对于正整数 N, 记

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) \mid c \equiv 0 \bmod N \right\}.$$

特别地, $\Gamma_0(1) = SL_2(\mathbb{Z})$.

如果上半平面 $\mathbb{H}$ 上的函数 $f(\tau)$ 满足以下条件：

(1) $f(\tau)$ 在 $\mathbb{H}$ 上是亚纯函数;

(2) $f(\tau)$ 在 $\Gamma_0(N)$ 作用下不变, 即 $f(\gamma\tau) = f(\tau), \gamma \in \Gamma_0(N)$, 此处作用即

$$\gamma(\tau) = \begin{pmatrix} a & b \\ c & d \end{pmatrix}(\tau) = \frac{a\tau + b}{c\tau + d}.$$

(3) $f(\tau)$ 在尖点处是亚纯的

则称 $f(\tau)$ 为 $\Gamma_0(N)$ 上的模函数.

由于任意格 $\Lambda = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$ 可以位似到 $\mathbb{Z} + \mathbb{Z}\tau$ 的形式, 其中 $\tau = \frac{\omega_1}{\omega_2}$ 的虚部大于 0. 则有：

定义 2.13　上半平面的 j-函数即 $\mathbb{H} \to \mathbb{C}; \tau \to j(E_{\Lambda_\tau})$, 其中 $\Lambda_\tau = \mathbb{Z} + \mathbb{Z}\tau$.

命题 2.8　j 函数满足

$$j(\tau) = j(-\frac{1}{\tau}),\ j(\tau) = j(\tau + 1),$$

故它在 $\mathrm{SL}_2(\mathbb{Z})$ 作用下保持不变, 即 $j(\gamma\tau) = j(\tau)$. 更进一步地, $j(\tau)$ 是 $\Gamma_0(1)$ 上的模函数.

证明　参考 [43] 定理 11.2. □

命题 2.9　设 $j_N(\tau) = j(N\tau)$, 则 $j_N(\tau)$ 是 $\Gamma_0(N)$ 上的模函数.

证明　参考 [43] 定理 11.9. □

定理 2.10　$\Gamma_0(N)$ 上的全体模函数组成了一个域, 它是有理函数域 $\mathbb{C}(j)$ 上由 j_N 生成的单扩张, 扩张次数是 $[\Gamma(1) : \Gamma_0(N)]$. 更进一步地, 设 $\Gamma(1)$ 关于 $\Gamma_0(N)$ 的一个右陪集表示是 $\{\gamma_1, \cdots, \gamma_n\}$, 则 j_N 的极小多项式为

$$\Phi_N(Y) = \prod_{i=1}^{n} (Y - j_N(\gamma_i\tau)). \tag{2.7}$$

证明　参考 [42] 定理 20.14 和 20.15. □

这里极小多项式的系数是在 $\mathbb{C}(j)$ 中, 如果我们考虑它作为 $\mathbb{C}$ 系数的多项式, 将 j 看成变量 X, 则有 $\Phi_N(X, Y) \in \mathbb{C}[X, Y]$. 很容易看出当 $X = j, Y = j_N$ 时, $\Phi_N(j, j_N) = 0$.

命题 2.11　函数 $\Phi_N(X,Y)$ 满足以下性质：

(1) 整性: $\Phi_N(X,Y) \in \mathbb{Z}(X,Y)$.

(2) 对称性：$\Phi_N(X,Y) = \Phi_N(Y,X)$.

(3) 以下设 ℓ 为一个素数, 则

$$\Phi_\ell(X,Y) = X^{\ell+1} + Y^{\ell+1} - X^\ell Y^\ell + \sum_{\substack{0\leqslant i,j\leqslant \ell \\ i+j<2\ell}} c_{ij} X^i Y^j. \tag{2.8}$$

(4) 两条椭圆曲线 E_1 和 E_2 通过 ℓ-同源 (即次数为 ℓ 的同源) 相连当且仅当 $\Phi_\ell(j(E_1), j(E_2)) = 0$.

(5) 设 j 为椭圆曲线 E 的 j-不变量. $E[\ell]$ 的所有 $\ell+1$ 个 ℓ 阶子群对应 $\ell+1$ 个 ℓ-同源, 这些同源连接的椭圆曲线的 j-不变量恰好是 $\Phi_\ell(j,Y)$ 的 $\ell+1$ 个根.

证明　参考 [42] 定理 20.17, 21.3, 21.4, 21.7;[43] 定理 11.18, 11.23. □

2.3.4　带复乘的椭圆曲线

对于复数域上的椭圆曲线 E, 如果其自同态环比整数环 $\mathbb{Z}$ 大, 则称椭圆曲线为带复乘的椭圆曲线.

在复数域上椭圆曲线的自同态环有两种情况：整数环 $\mathbb{Z}$ 或者虚二次域的序. 后者称为是带复乘的.

2.3.5　带复乘的椭圆曲线和类域

定义 2.14　若 $\mathcal{O}$ 为虚二次域的序, 且有判别式 D, 记

$$\mathrm{Ell}_{\mathcal{O}}(\mathbb{C}) = \{j(E) \in \mathbb{C} \mid \mathrm{End}(E) = \mathcal{O}\}.$$

定义 2.15　Hilbert 类多项式即

$$H_D(X) = \prod_{j(E)\in \mathrm{Ell}_{\mathcal{O}}(\mathbb{C})} (X - j(E)). \tag{2.9}$$

定理 2.12　设 $\mathcal{O}$ 是虚二次域 K 的序, $\mathrm{disc}(\mathcal{O}) = D$, 且 $j \in \mathrm{Ell}_{\mathcal{O}}(\mathbb{C})$. 则 Hilbert 类多项式 $H_D(X)$ 是次数是 $\mathcal{O}$ 的类数 $h(\mathcal{O})$ 的整系数不可约多项式.

证明　证明参考 [43] 定理 11.1. □

定义 2.16　对于固定的椭圆曲线 E, 记 $E_I = E/E[I]$, 其中

$$E[I] = \{P \in E(\mathbb{C}) \mid \alpha(P) = \mathcal{O}, \forall \alpha \in I\}.$$

设 $L = K(j(E))(E \in \mathrm{Ell}_{\mathcal{O}}(\mathbb{C}))$ 是 $\mathcal{O}$ 的环类域, 则 $\mathrm{Gal}(L/K)$ 和类群 $\mathrm{Cl}(\mathcal{O})$ 在 $\mathrm{Ell}_{\mathcal{O}}(\mathbb{C})$ 上有作用：

$$\mathrm{Gal}(L/K) \times \mathrm{Ell}_{\mathcal{O}}(\mathbb{C}) \to \mathrm{Ell}_{\mathcal{O}}(\mathbb{C});\ (\sigma, j) \mapsto \sigma(j);$$

$$\mathrm{Cl}(\mathcal{O}) \times \mathrm{Ell}_{\mathcal{O}}(\mathbb{C}) \to \mathrm{Ell}_{\mathcal{O}}(\mathbb{C});\ ([I], j(E_J)) \mapsto E_{I^{-1}J}.$$

定理 2.13　存在典范同构 $\mathrm{Gal}(L/K) \cong \mathrm{Cl}(\mathcal{O})$, 保持 $\mathrm{Ell}_{\mathcal{O}}(\mathbb{C})$ 上的作用, 且上述作用是可迁和自由的.

证明　证明参考 [42] 定理 22.1 和推论 22.2. □

2.3.6　带复乘的复椭圆曲线之间的同源

定理 2.14　设 E_1, E_2 为 $\mathbb{C}$ 上的带复乘的椭圆曲线, $\phi : E_1 \to E_2$ 为次数 ℓ 的同源. 则：

(1) $\mathrm{End}(E_1) \bigotimes \mathbb{Q} \cong \mathrm{End}(E_2) \bigotimes \mathbb{Q}$, 记此虚二次域为 K.

(2) 记 $\mathrm{End}(E_1) = \mathcal{O}_1, \mathrm{End}(E_2) = \mathcal{O}_2$. 它们都是虚二次域 K 上的序, 则以下情况之一成立:

(i) $\mathcal{O}_1 = \mathcal{O}_2$, 此时称 ϕ 为水平的;

(ii) $[\mathcal{O}_1 : \mathcal{O}_2] = \ell$, 此时称 ϕ 为下降的;

(iii) $[\mathcal{O}_2 : \mathcal{O}_1] = \ell$, 此时称 ϕ 为上升的.

证明　参考 [42] 定理 23.3 和定义 23.4. □

定理 2.15　设 E 为 $\mathbb{C}$ 上的带复乘的椭圆曲线, 它的自同态环 $\mathcal{O}$ 是虚二次域 K 的判别式为 D 的序. 设 ℓ 为一个素数, 则：

(1) 当 $\ell \nmid [\mathcal{O}_K : \mathcal{O}]$ 时, 从 E 出发的 $\ell + 1$ 个 ℓ-同源中,

(i) $1 - (\frac{D}{\ell})$ 个是水平的同源;

(ii) $\ell + (\frac{D}{\ell})$ 个是下降的同源;

(iii) 0 个是上升的同源.

(2) 当 $\ell \mid [\mathcal{O}_K : \mathcal{O}]$ 时, 从 E 出发的 $\ell + 1$ 个 ℓ-同源中,

(i) 0 个是水平的同源;

(ii) ℓ 个是下降的同源;

(iii) 1 个是上升的同源.

证明　证明参考 [42] 定理 23.5. □

2.4　有限域上的椭圆曲线

定义 2.17　记 E 为有限域 $\mathbb{F}_q$ 上的椭圆曲线, 其中 $q = p^n$. 记

$$\pi : E \to E; (x, y) \to (x^{p^n}, y^{p^n})$$

是有限域上椭圆曲线的 Frobenius 映射. 则 π 的极小多项式是:

$$x^2 - tx + q, \tag{2.10}$$

其中 $t = \mathrm{tr}(\pi) = \pi + \hat{\pi}$.

定理 2.16　(Hasse) 设 E 为有限域 $\mathbb{F}_q$ 上椭圆曲线. 它的有理点个数与 t 满足

$$t = q + 1 - \#E(\mathbb{F}_q) \tag{2.11}$$

且

$$|t| \leqslant 2\sqrt{q}. \tag{2.12}$$

证明　证明参考 [40] 第五章定理 1.1.　□

定理 2.17　(Tate) 设 E_1, E_2 为有限域 $\mathbb{F}_q$ 上的椭圆曲线. 则存在定义在 $\mathbb{F}_q$ 上的同源 $\phi : E_1 \to E_2$ 当且仅当 $\#E_1(\mathbb{F}_q) = \#E_2(\mathbb{F}_q)$.

证明　证明参考 [44].　□

定义 2.18　有限域上椭圆曲线 E 的 m 阶挠点 $E[m] = \ker([m]) = \{P \in E(\overline{K}) \mid mP = O\}$.

定理 2.18　当 $p \nmid m$ 时, $E[m] \cong (\mathbb{Z}/m\mathbb{Z})^2$. 对于 $r \geqslant 1$, $E[p^r]$ 有两种情况, 或者 $E[p^r] = 0$ 对任意 r 同时成立, 或者 $E[p^r] = \mathbb{Z}/p^r\mathbb{Z}$.

证明　可以参考 [40] 第三章推论 6.4.　□

定义 2.19　考虑同源 $\phi : E_1 \to E_2$, 若 $\overline{K}(E_1)$ 是 $\phi^*(\overline{K}(E_2))$ 的可分 ((纯) 不可分) 扩张, 则称 ϕ 是可分 ((纯) 不可分) 的.

特别地, 当 $p \nmid \deg(\phi)$ 时 ϕ 是可分扩张, 而 Frobenius 映射 π 是纯不可分扩张.

有限域上的椭圆曲线之间存在同源也可以用模多项式刻画：

命题 2.19　E_1 和 E_2 是有限域 $\mathbb{F}_q (q = p^n)$ 上的两条椭圆曲线, E_1 和 E_2 通过 ℓ-同源相连当且仅当在 $\mathbb{F}_q$ 中 $\Phi_\ell(j(E_1), j(E_2)) = 0$.

2.4.1　正常和超奇异椭圆曲线

定义 2.20　对于有限域上的椭圆曲线 E, 若 $E[p^r] = 0$, 则称 E 为超奇异 (supersingular) 的; 若 $E[p^r] = \mathbb{Z}/p^r\mathbb{Z}$, 则称 E 为正常 (ordinary) 的.

当然我们还有其他的判别方法, 判断椭圆曲线是不是超奇异椭圆曲线：

定理 2.20　设 E 是有限域 $\mathbb{F}_{p^n}$ 上的椭圆曲线, 定义 $\phi_r : E \to E^{(p^r)}$ 为 p^r 次 Frobenius 映射, $\hat{\phi}_r$ 为其对偶. 则下列条件均等价：

(1) $E[p^r] = 0$ 对于任意 $r \geqslant 1$ 成立;

(2) $\hat{\phi}_r$ 为纯不可分的, 对于任意 $r \geqslant 1$ 成立;

(3) $[p]$ 是纯不可分的, 且 $j(E) \in \mathbb{F}_{p^2}$;

(4) $\mathrm{End}(E)$ 为四元数代数的极大序;

(5) E 的 Hasse 不变量等于 0;

(6) $p \mid t = \mathrm{tr}(\pi)$.

证明　证明参考 [40] 第五章定理 3.1. □

对应地, 我们有正常椭圆曲线的判别方法：

定理 2.21　设 E 为有限域 $\mathbb{F}_{p^n}$ 上的椭圆曲线. 则下列条件等价：

(1) $E[p^r] = \mathbb{Z}/p^r\mathbb{Z}$ 对于任意 $r \geqslant 1$ 成立;

(2) $\hat{\phi}_r$ 不是纯不可分的, 对于任意 $r \geqslant 1$ 成立;

(3) $[p]$ 不是纯不可分的, 且 $j(E)$ 在 $\mathbb{F}_p$ 上超越;

(4) $\mathrm{End}(E)$ 为虚二次域的序;

(5) E 的 Hasse 不变量为 1;

(6) $p \nmid t = \mathrm{tr}(\pi)$.

证明　证明参考 [40] 第五章定理 3.1. □

对于有限域 $\mathbb{F}_{p^n}$ 上的椭圆曲线 E 的 Frobenius 映射的迹, 有下面的结果：

定理 2.22　对于 E 为有限域 $\mathbb{F}_q$ 上的椭圆曲线 ($q = p^n$), 定义 π 为 Frobenius 映射, $t = \mathrm{tr}(\pi)$, 则 t 满足下述情况之一：

(1) $p \nmid t, t^2 \leqslant 4q$;

(2) n 为奇数, $t = 0$;

(3) n 为奇数, $t = \pm\sqrt{2q}$, $p = 2$;

(4) n 为奇数, $t = \pm\sqrt{3q}$, $p = 3$;

(5) n 为偶数, $t = \pm 2\sqrt{q}$;

(6) n 为偶数, $t = \pm\sqrt{q}$, $p \not\equiv 1 \bmod 3$;

(7) n 为偶数, $t = 0$, $p \not\equiv 1 \bmod 4$.

证明　证明参考 [45] 第五章定理 3.1. □

当 j 是 0 和 1728 时：

定理 2.23　(1) j 不变量是 1728 的椭圆曲线是超奇异椭圆曲线当且仅当 $p \equiv 3 \bmod 4$.

(2) j 不变量是 0 的椭圆曲线是超奇异椭圆曲线当且仅当 $p \equiv 2 \bmod 3$.

证明　证明参考 [40] 第五章例子 4.4, 4.5. □

2.4.2　有限域上椭圆曲线的自同态环

对于有限域 $\mathbb{F}_{p^n}$ 上的椭圆曲线 E 的自同态环有下面结果.

定理 2.24　设 E 为有限域 $\mathbb{F}_q$ 上的椭圆曲线 ($q = p^n$), 定义 π 为 Frobenius 映射, $t = \mathrm{tr}(\pi)$. 则有以下情况：

(1) 若 E 为正常椭圆曲线, 即 $p \nmid t$, 则 $\mathrm{End}(E) = \mathrm{End}_{\mathbb{F}_q}(E)$ 为虚二次域的序.

(2) 若 E 为超奇异椭圆曲线且 $t \neq \pm 2\sqrt{q}$, 则 $\mathrm{End}(E)$ 是只在 p 与 ∞ 处分歧的四元数代数 $B_{p,\infty}$ 的极大序, $\mathrm{End}_{\mathbb{F}_q}(E)$ 为虚二次域的序.

(3) 若 E 为超奇异椭圆曲线且 $t = \pm 2\sqrt{q}$, 则 $\mathrm{End}(E) = \mathrm{End}_{\mathbb{F}_q}(E)$ 是只在 p 与 ∞ 处分歧的四元数代数 $B_{p,\infty}$ 的极大序.

证明　证明参考 [45] 定理 4.3 或者 [46]. □

2.5　四元数代数及其与椭圆曲线

由于有限域上超奇异椭圆曲线的自同态环是四元数代数的极大序, 所以我们需要四元数代数一些结果. 这部分结果可以参考 [47].

2.5.1　四元数代数

定义 2.21　域 F 上的四元数代数是一个四维的 F 代数, 有一组基是 $1, i, j, k$, 满足条件 $i^2 = -a, j^2 = -b, ij = -ji = k (a, b \in F^\times)$. 它通常记为为 $(\frac{a,b}{F})$.

四元数代数是非交换的代数. 由维德伯恩定理, 四元数代数或者是中心可除代数或者同构于 $M_2(F)$. 由于考虑的是椭圆曲线自同态环, 我们之后都假设域 F 是有理数域 $\mathbb{Q}$.

定义 2.22　如果 $B_p = B \bigotimes \mathbb{Q}_p$ 是可除代数, 称 B 在 p 处分歧; 如果 $B_p = B \bigotimes \mathbb{Q}_p \cong M_2(\mathbb{Q}_p)$, 称 B 在 p 处分裂.

记 $B = B_{p,\infty}$ 为只在 p 和无穷处分歧的四元数 $\mathbb{Q}$-代数.

$B_{p,\infty}$ 是超奇异椭圆曲线自同态环所在的代数, 是我们重点考虑的对象.

定义 2.23　四元数代数 $B = (\frac{a,b}{\mathbb{Q}})$ 上的对合映射即

$$\iota : B \to B; \quad \alpha = x + yi + zj + wk \to \bar{\alpha} = x - yi - zj - wk.$$

四元数 $\alpha = x + yi + zj + wk$ 的约化迹和约化范数分别是

$$\mathrm{Trd}(\alpha) = \alpha + \bar{\alpha} = 2x, \ \ \mathrm{Nrd}(\alpha) = \alpha\bar{\alpha} = x^2 + ay^2 + bz^2 + abw^2. \tag{2.13}$$

定义 2.24　若 Λ 是四元数代数 B 的 $\mathbb{Z}$-子模, 且 Λ 包含 B 的一组 $\mathbb{Q}$-基, 则称 Λ 是 B 的一个格,

更进一步地, 若 Λ 还是 B 的一个子环, 则称 Λ 为 B 的一个序. 若 Λ 是 B 的极大的序, 即不真包含于其他序, 则称 Λ 是 B 的极大序.

定义 2.25　设 $\mathcal{O}$ 是四元数代数 B 的一个极大序. 设 I 是 $\mathcal{O}$ 的左理想. I 的左序定义为

$$\mathcal{O}_L(I) = \{x \in B \mid xI \subseteq I\}.$$

右序定义为

$$\mathcal{O}_R(I) = \{x \in B \mid Ix \subseteq I\}.$$

I 的约化范数定义为

$$\mathrm{Nrd}(I) = \gcd\{\mathrm{Nrd}(\alpha) : \alpha \in I\}.$$

共轭理想定义为

$$\bar{I} = \{\bar{\alpha} : \alpha \in I\}.$$

两个左理想 I 和 J 等价是指存在 $\mu \in B^\times$ 使得 $J = I\mu$.

命题 2.25　设 $\mathcal{O}$ 是 $B = B_{p,\infty}$ 的一个极大序. 则

(1) $\mathrm{disc}(B_{p,\infty}) = p$.

(2) 两个极大序 $\mathcal{O}, \mathcal{O}'$ 同构当且仅当存在 $\mu \in B_{p,\infty}^\times$ 使得 $\mathcal{O}' = \mu\mathcal{O}\mu^{-1}$.

(3) 设 I 是左理想. 则 $\mathcal{O}_L(I) = \mathcal{O}$, 且 $\mathcal{O}_R(I)$ 也为 B 的一个极大序.

(4) 设 I 是左理想, 则

$$I\bar{I} = \mathrm{Nrd}(I)\mathcal{O} = \mathrm{Nrd}(I)\mathcal{O}_R(\bar{I}), \quad \bar{I}I = \mathrm{Nrd}(I)\mathcal{O}_L(\bar{I}). \tag{2.14}$$

证明　证明参考 [47] 第 42 章. □

引理 2.26　若 $\mathcal{O}$ 为 $B_{p,\infty}$ 的极大序, 左 $\mathcal{O}$ 理想 I 约化范数是 ℓ, 则 $\ell \in I$.

证明　由于阿贝尔群 $\mathcal{O}/I$ 的阶为 $\mathrm{Nrd}(I)^2 = \ell^2$. 若 $\ell \notin I$. 则 1 在 $\mathcal{O}/I$ 中的像的阶数为 ℓ^2, 从而 $\mathcal{O}/I \cong \mathbb{Z}/\ell^2\mathbb{Z}$ 为一个循环群.

令 $\{1, a, b, c\}$ 为 $\mathcal{O}$ 的一组 $\mathbb{Z}$-基. 令 $t_a, t_b, t_c \in \mathbb{Z}$ 使得 $a - t_a, b - t_b, c - t_c \in I$. 我们用 $\{a, b, c\}$ 来代替 $\{a - t_a, b - t_b, c - t_c\}$, 则我们得到了 $\mathcal{O}$ 的一组 $\mathbb{Z}$-基：$\{1, a, b, c\}$ 使得 $\{\ell^2, a, b, c\}$ 为 I 的一组 $\mathbb{Z}$-基.

通过计算可得, $\mathcal{O} \subseteq \mathcal{O}_R(I)$, 又它们都为 $B_{p,\infty}$ 的极大序, 从而 $\mathcal{O}_L(I) = \mathcal{O} = \mathcal{O}_R(I)$. 由命题 2.25可知

$$\bar{I}I = \ell\mathcal{O}_R(I), I\bar{I} = \ell\mathcal{O}_L(I).$$

由此 $\bar{I}I = \ell\mathcal{O} \subseteq \mathcal{O}$, 且由定义 $\bar{I} \subseteq \mathcal{O}_L(I) = \mathcal{O}$. 从而, $\ell\mathcal{O} = \bar{I}I \subseteq \mathcal{O}I \subseteq I$. 得出矛盾, 即证. □

2.5.2　Deuring 对应

设 E 是 $\mathbb{F}_{p^2}$ 上的超奇异椭圆曲线, 则 $\mathcal{O}=\mathrm{End}(E)$ 是 $B_{p,\infty}$ 的极大序, I 为 $\mathcal{O}$ 的左理想, 设 n 与 p 互素. 设 I 是 $\mathcal{O}$ 的左理想, 其约化范数 $\mathrm{Nrd}(I)=n$. 记

$$E[I]=\{P\in E(\overline{\mathbb{F}_p}) \mid \alpha(P)=O, \forall \alpha\in I\}.$$

则 $E[I]$ 是 $E(\overline{\mathbb{F}_p})$ 的有限子群. 从而存在同源:

$$\phi_I : E\to E_I=E/E[I],$$

使得 $\ker(\phi_I)=E[I]$. 反之, 若同源 $\phi_I : E\to E'$ 的次数是 n, 定义

$$I_\phi=\{\alpha\in\mathcal{O} \mid \alpha(P)=O, \forall P\in\ker(\phi)\}.$$

则 I_ϕ 是约化范数为 n 的 $\mathcal{O}$ 的左理想.

Deuring 对应定理是如下定理:

定理 2.27　(Deuring 对应) 若 E 是 $\mathbb{F}_{p^2}$ 上的超奇异椭圆曲线, 则 $\mathcal{O}=\mathrm{End}(E)$ 是 $B_{p,\infty}$ 上的极大序, 且

(1) $\mathcal{O}$ 的约化范数是 n 的左理想 I 以下述对应一一对应到次数是 n 的同源 $\phi : E\to E'$ 的同构类:

$$I\mapsto[\phi_I];\quad [\phi]\mapsto I_\phi.$$

(2) 在此对应下, $\mathrm{End}(E')\cong\mathcal{O}_R(I)$ 是 I 在 $B_{p,\infty}$ 中的右序. 特别地，$\phi\in\mathrm{End}(E)$ 当且仅当 $I=I_\phi=\mathcal{O}\phi$ 是主理想.

(3) 若 $\phi_1 : E\to E_1, \phi_2 : E\to E_2$ 为对应 $I_1, I_2\subseteq\mathcal{O}$ 的两个同源. 则 E_1 与 E_2 同构当且仅当 $I_1=I_2x$, 其中 $x\in B_{p,\infty}^\times$, 即 I_1，I_2 在同一个左理想类中.

证明　证明参考 [47] 第 42 章. □

2.5.3　超奇异椭圆曲线自同态环具体形式

由 [48], [27], [28] 知, 超奇异椭圆曲线的自同态环为:

命题 2.28　设 E 是 $j(E)=j$ 的超奇异椭圆曲线.

(1) 当 $j=1728$ 时,

$$\mathrm{End}(E_{1728})=\mathbb{Z}+\mathbb{Z}i+\mathbb{Z}\frac{1+j}{2}+\mathbb{Z}\frac{i+k}{2},$$

其中 $i^2=-1, j^2=-p, ij=-ji=k$.

(2) 当 $j=0$ 时,

$$\mathrm{End}(E_0)=\mathbb{Z}+\mathbb{Z}\frac{1+i}{2}+\mathbb{Z}\frac{i+k}{3}+\mathbb{Z}\frac{j+k}{2},$$

其中 $i^2=-3$, $j^2=-p$, $ij=-ji=k$. 它也可以写

$$\mathrm{End}(E_0)=\mathbb{Z}+\mathbb{Z}\frac{-1+i}{2}+\mathbb{Z}j+\mathbb{Z}\frac{3+i+3j+k}{6},$$

其中 $i^2=-3$, $j^2=-p$, $ij=-ji=k$.

(3) 当 $j\in\mathbb{F}_p$ 时, 若 $\frac{1+\pi}{2}\notin\mathrm{End}(E)$,

$$\mathrm{End}(E)=\mathbb{Z}+\mathbb{Z}\frac{1+i}{2}+\mathbb{Z}\frac{j-k}{2}+\mathbb{Z}\frac{ri-k}{q},$$

其中 $(\frac{p}{q})=-1$, $q\equiv 3 \bmod 8$, $r^2\equiv -p \bmod q$, $i^2=-q$, $j^2=-p$, $ij=-ji=k$.

(4) 当 $j\in\mathbb{F}_p$ 时, 若 $\frac{1+\pi}{2}\in\mathrm{End}(E)$,

$$\mathrm{End}(E)=\mathbb{Z}+\mathbb{Z}\frac{1+j}{2}+\mathbb{Z}i+\mathbb{Z}\frac{r'i-k}{2q},$$

其中 $(\frac{p}{q})=-1$, $q\equiv 3 \bmod 8$, $r'^2\equiv -p \bmod 4q$, $i^2=-q$, $j^2=-p$, $ij=-ji=k$.

第 3 章　阿贝尔簇基础知识

3.1　除子, 可逆层, 线丛

在这里我们考虑域 K 上的非奇异 (光滑) 簇 X.

3.1.1　除子

定义 3.1　对于域 K 上的簇 X, 我们有以下定义：

(1) Weil 除子群是由余维数是 1 的闭子簇生成的自由阿贝尔群, 即

$$\mathrm{Div}(X) = \{D = \sum_Y n_Y Y\},$$

其中 Y 为 X 的余维数为 1 的闭子簇 (素除子), 且只有有限个 n_Y 不为 0. D 称为除子. 若所有的 $n_Y \geqslant 0$, 则称该除子是有效除子, 记为 $D \geqslant 0$.

(2) 除子 D 的次数定义为:

$$\deg(D) = \sum_Y n_Y.$$

(3) 主除子群即

$$\mathrm{Pri}(X) = \{(f) = \sum_Y v_Y(f)Y \mid f \in K(X)\},$$

其中 $v_Y(f)$ 是在 Y 处赋值, (f) 称为 f 对应的主除子.

(4) 除子类群即

$$\mathrm{Cl}(X) = \mathrm{Div}(X)/\mathrm{Pri}(X).$$

定义 3.2　(1) Cartier 除子. 若 $(U_i, f_i)_{i\in I}$ 满足:

(i) U_i 为 X 的开覆盖,

(ii) f_i 为非 0 的有理函数, 即 $f_i \in k(U_i)^*$,

(iii) $f_i f_j^{-1} \in \mathcal{O}(U_i \cap U_j)^*$, 即 $f_i f_j^{-1}$ 在 $U_i \cap U_j$ 上没有零点和极点,

则称其为一个 Cartier 除子. 对于 Cartier 除子 $\{(U_i, f_i)_{i\in I}\}$, 若 $f_i \in \mathcal{O}(U_i)$, 则称其为有效除子. 全体 Cartier 除子记为 $\mathrm{CaDiv}(X)$.

(2) 两个 Cartier 除子 $\{(U_i, f_i)_{i\in I}\}, \{(V_j, g_j)_{j\in J}\}$ 等价是指 $f_i g_j^{-1} \in \mathcal{O}(U_i \cap V_j)^\times$ 对于任意的 $i \in I$ 和 $j \in J$ 成立.

(3) Cartier 除子的加法是

$$\{(U_i, f_i)_{i\in I}\} + \{(V_j, g_j)_{j\in J}\} = \{(U_i \cap V_j, f_i g_j)_{(i,j)\in I\times J}\}.$$

(4) 主除子即除子

$$\mathrm{div}(f) = \{(X, f)\}.$$

所有主除子的集合是 $\mathrm{Pri}(X)$.

(5) 除子类群:

$$\mathrm{CaCl}(X) = \mathrm{CaDiv}(X)/\mathrm{Pri}(X).$$

定理 3.1　在非奇异簇的情况下, Weil 除子和 Cartier 除子一一对应, 即

$$\mathrm{Cl}(X) \cong \mathrm{CaCl}(X).$$

证明　证明参考 [49] 第二章命题 6.11. □

3.1.2　可逆层

定义 3.3　可逆层是秩 1 的局部自由层. 以张量积作为乘法, 可逆层集合构成乘法群, 称为 Picard 群 $\mathrm{Pic}(X)$.

对于 X 上的 Cartier 除子 $D = \{(U_i, f_i)_{i\in I}\}$, 定义可逆层 $\mathscr{L}(D)$ 为在 U_i 上由 ${f_i}^{-1}$ 生成的自由 $\mathcal{O}_X$ 模, 称 $\mathscr{L}(D)$ 为和 D 相伴的可逆层.

定理 3.2　在非奇异簇的情况下, Cartier 除子和可逆层有一一对应的关系: $D \to \mathscr{L}(D)$, 即

$$\mathrm{Cl}(X) \cong \mathrm{CaCl}(X) \cong \mathrm{Pic}(X).$$

证明　证明参考 [49] 第二章命题 6.15. □

3.1.3　强可逆层和射影态射

定义 3.4　X 上的可逆层 $\mathscr{L}$ 称为极强的, 若存在一个浸没 $i : X \to \mathbb{P}^r_K$, 使得 $i^*(\mathcal{O}(1)) \cong \mathscr{L}$.

X 上的可逆层 $\mathscr{L}$ 是强的, 若对于 X 上的每个凝聚层 $\mathcal{F}$, 存在正整数 n_0 使得对于每个 $n \geqslant n_0$, $\mathscr{L}^n \bigotimes \mathcal{F}$ 由整体截面生成.

定理 3.3　(Serre) 若 X 上的可逆层 $\mathscr{L}$ 是极强的，则 $\mathscr{L}$ 是强的.

另一方面, 若 $\mathscr{L}$ 是强的, 存在正整数 m 使得 $\mathscr{L}^m$ 是极强的.

证明　证明参考 [49] 第二章命题 7.5, 7.6. □

定理 3.4　对于 $\phi : X \to \mathbb{P}^n$ 为 K 上的态射, 则 $\phi^*(\mathcal{O}(1))$ 为 X 上的可逆层, 并由整体截面 $s_i = \phi^*(x_i)$ 生成.

另一方面, 如果 $\mathscr{L}$ 是 X 上可逆层, 且由整体截面 $s_0, \cdots, s_n \in \mathscr{L}(X)$ 生成, 则存在唯一的态射 $\phi : X \to \mathbb{P}^n$, 使得 $\mathscr{L} \cong \phi^*(\mathcal{O}(1))$, 且有 $s_i = \phi^*(x_i)$.

证明　证明参考 [49] 第二章命题 7.1. □

3.1.4　线性系

定义 3.5　对于可逆层 $\mathscr{L}$, $s \in \mathscr{L}(X)$, 定义 s 的零点除子 $(s)_0$ 为 Cartier 除子 $(U, \phi(s))$, 其中 ϕ 为在 U 上 $\mathscr{L}$ 和 $\mathcal{O}_X$ 的同构.

定义 3.6　给定除子 D, 线性空间

$$L(D)(X) = \{f \in K(X) \mid (f) + D \geqslant 0\} \cup \{0\},$$

维数定义为 $l(D)$.

定义 3.7　对于除子 D_0, 所有线性等价于 D_0 的有效除子集合称为一个完全线性系, 记为 $|D_0|$.

完全线性系一一对应到:

$$(\mathscr{L} - \{0\})/K^*,$$

即

$$(L(D)(X) - \{0\})/K^*.$$

定义 3.8　线性系 σ 是完全线性系的子集, 且在射影空间结构下是线性空间, 对应线性空间 $V = \{s \in \mathscr{L}(X) \mid (s)_0 \in \sigma\}$, 从而 $\dim \sigma = \dim V - 1$.

线性系 σ 的基点：若对于任意的 $D \in \sigma$, 有 $P \in \mathrm{Supp}(D)$, 则称 P 为 σ 的基点.

定理 3.5　(1) 给定一个态射 $\phi : X \to \mathbb{P}^n$ 就等价于给定一个无基点的线性系 σ.

(2) 若还要 ϕ 是闭浸入则需要：

(i) σ 分离点：对于任意的 $P, Q \in X$, 存在 $D \in \sigma$, 使得 $P \in \mathrm{Supp}(D)$, $Q \notin \mathrm{Supp}(D)$.

(ii) σ 分离切向量：给定点 P 和 P 点处的切向量 t, 存在 $D \in \sigma$, 使得 $P \in \mathrm{Supp}(D)$, $t \notin T_P(D)$.

证明　证明参考 [49] 第二章命题 7.8, 注 7.8.2. □

3.1.5　线丛

定义 3.9　簇 E 为 X 上的线丛：存在 $p : E \to X$, 使得

(1) $p^{-1}(X)$ 为一维线性空间

(2) 对于任意的 $x \in X$, 存在 x 的开邻域 U, 使得 $\phi_U : E|_U \to U \times \mathbb{A}^1$ 为同构, 而且有 $p = p_1 \circ \phi_U$, 其中 p_1 为第一分量投射.

定义 3.10　线丛 E 对应的可逆层 $\mathscr{L}(E)$ 即

$$\mathscr{L}(E)(U) = \{s : U \to E \mid p \circ s = 1\}$$

则有下面的结果

定理 3.6　线丛和可逆层有一一对应的关系：

$$E \to \mathscr{L}(E).$$

证明　证明参考 [50] 定理 A.3.3.4. □

综上所述, 在接下来的讨论中我们将 Weil 除子, Cartier 除子, 可逆层, 线丛看作是相同的概念.

3.2　代数曲线

3.2.1　在射影空间中的嵌入

定理 3.7　对于曲线 C 上的除子 D,

(1) D 是无基点的当且仅当对于任意的 $P \in C$, 有:

$$l(D-P) = l(D) - 1; \tag{3.1}$$

(2) D 是极强的当且仅当对于任意的 $P, Q \in C$, 有:

$$l(D-P-Q) = l(D) - 2. \tag{3.2}$$

证明　证明参考 [49] 第四章命题 3.1. □

上面的定理第一条结果给了到射影空间存在态射的充要条件, 第二条给了该态射是闭浸入的充要条件.

3.2.2　黎曼-洛赫定理

定理 3.8　(黎曼-洛赫定理) 对于曲线 C 上的除子 D 有：

$$l(D) - l(K_X - D) = \deg(D) - g + 1, \tag{3.3}$$

其中 K_X 为由微分定义的典范除子, g 为曲线的亏格.

证明　证明参考 [49] 第四章定理 1.3. □

黎曼-洛赫定理有以下推论：

推论 3.9　设 C 是亏格 g 的曲线.

(1) $l(K_X) = g, \deg(K_X) = 2g - 2$.

(2) 当 $\deg(D) \geqslant 2g$ 时, D 无基点.

(3) 当 $\deg(D) \geqslant 2g + 1$ 时, D 极强.

(4) D 为强的当且仅当 $\deg(D) > 0$.

证明　证明参考 [49] 第四章系 3.2, 3.3. □

3.3　超椭圆曲线

3.3.1　超椭圆曲线的定义

定义 3.11　超椭圆曲线 C 是亏格 $\geqslant 2$ 的非奇异曲线且存在一个二次有限态射 $f : C \to \mathbb{P}^1$.

当代数曲线的亏格 $g = 2$ 时, 它的典范除子 K_X 是 $\deg = 2g - 2 = 2$ 的除子, 由黎曼-洛赫定理可以算出 K 对应一维无基点线性系, 这样就给出了射影态射 $f : C \to \mathbb{P}^1$, 从而亏格是 2 的非奇异曲线都是超椭圆曲线. 当亏格 $\geqslant 3$ 时才有非超椭圆曲线的例子.

3.3.2　超椭圆曲线的方程

和椭圆曲线一样通过计算扩张次数和对应的阶, 我们可以得到超椭圆曲线的方程：当域的特征不为 2 和 3 时, $y^2 = f(x)$, 其中 $f(x)$ 为次数为 $2g+1$ 或者 $2g+2$ 的首一多项式 (g 为曲线亏格), 若要求非奇异性则要求 $f(x)$ 无重根.

定义 3.12　超椭圆对合即态射

$$\iota : C \to C; (x, y) \to (x, -y). \tag{3.4}$$

对于 $P = (x_P, y_P)$, 若 $P = \iota(P)$, 则一致化参数是 $y - y_P$, $\upsilon_P(x - x_P) = 2$; 若 $P \neq \iota(P)$, 则一致化参数是 $x - x_P$.

由于密码学中现阶段使用的主要是亏格 2 的超椭圆曲线, 所以我们接下来考虑亏格为 2 的超椭圆曲线.

3.3.3　亏格 2 的超椭圆曲线上的不变量

定义 3.13　对于超椭圆曲线

$$C : y^2 = f(x) = (x - x_1) \cdots (x - x_6),$$

定义 $(ij) = x_i - x_j$, 则有不变量:

- $I_2 = \sum (12)^2 (34)^2 (56)^2$,
- $I_4 = \sum (12)^2 (23)^2 (31)^2 (45)^2 (64)^2 (56)^2$,
- $I_6 = \sum (12)^2 (23)^2 (31)^2 (45)^2 (64)^2 (56)^2 (14)^2 (25)^2 (36)^2$,
- $I_{10} = \sum (12)^2$,

称为 Igusa-Clebsch 不变量.

定理 3.10　若超椭圆曲线 C 的不变量是 $[I_2, I_4, I_6, I_{10}]$, C' 的不变量是 $[I_2', I_4', I_6', I_{10}']$, 则 C 和 C' 同构当且仅当存在 $\lambda \in \overline{K}^{\times}$, 使得

$$[I_2', I_4', I_6', I_{10}'] = [\lambda^2 I_2, \lambda^4 I_4, \lambda^6 I_6, \lambda^{10} I_{10}].$$

证明　可以参考 [51] 632 页. □

3.3.4　亏格 2 的超椭圆曲线上的除子 Munford 表示

这部分可以参考 [52] 第十章第三节.

定义 3.14　对于超椭圆曲线 C 上的有效除子 $D = \sum n_P P$, 如果满足：

(1) 若 $P = \iota(P)$, 则 $n_P = 1$.

(2) 若 $P \neq \iota(P)$, 则 $n_P > 0$ 推出 $n_{\iota(P)} = 0$.

则称除子 D 是半约化除子.

超椭圆曲线的任一除子都可以等价于一个半约化除子.

定义 3.15　Mumford 表示：对于超椭圆曲线 C 上的除子可以等价到半约化除子: 对于除子

$$D = \sum_i e_i(x_i, y_i).$$

令 $u(x) = \prod_i (x - x_i)^{e_i}$, 可找到唯一的 $v(x)$ 使得 $v(x_i) = y_i$, $\deg(v(x)) < \deg(u(x))$, 且 $v(x)^2 \equiv f(x) \bmod u(x)$. 那么可以用 $(u(x), v(x))$ 表示除子 D, 即:

$$D = \sum_i e_i(x_i, v(x_i)).$$

(这里 $\deg(u(x)) \leqslant g$)

命题 3.11　对于亏格 2 的超椭圆曲线 C, 则 $\deg(u(x)) \leqslant 2$, 故两种情况：

(1) $\deg(u(x)) = 1$, 则 $P = (x_1, y_1)$ 为唯一的点在 $\mathrm{Supp}(D)$ 中, 从而

$$u(x) = (x - x_1), v(x) = y_1.$$

Mumford 表示为:

$$(x - x_1, y_1).$$

(2) $\deg(u(x)) = 2$, 则 $P = (x_1, y_1)$, $Q = (x_2, y_2)$ 在 $\mathrm{Supp}(D)$ 中 $(x_1 \neq x_2)$, 从而

$$u(x) = (x - x_1)(x - x_2) = x^2 + u_1 x + u_0 (u_1 = -x_1 - x_2, u_0 = x_1 x_2),$$

$$v(x) = v_1 x + v_0 (v_1 = \frac{y_2 - y_1}{x_2 - x_1}, v_0 = \frac{y_1 x_2 - x_1 y_2}{x_2 - x_1}).$$

Mumford 表示为:

$$(x^2 + u_1 x + u_0, v_1 x + v_0).$$

证明　可以参考 [52] 第十章第三节. □

同样的在超椭圆曲线上可以定义加法.

3.4　复数域上的阿贝尔簇

3.4.1　复数域上的阿贝尔簇

这部分结果可以参考 [50]A.5, A.6.

复数域上的复环面是 $\mathbb{C}^g/\Lambda$ 的形式, 其中 Λ 是 $\mathbb{C}^g$ 中的格, 但不是所有复环面都是射影的 (即有强的线丛).

定义 3.16　黎曼型 (厄密特形式)：$H : \mathbb{C}^g \times \mathbb{C}^g \to \mathbb{C}$ 是一个厄密特型, 且 $H : \Lambda \times \Lambda \to \mathbb{Z}$.

黎曼型 (反对称形式): $E : \mathbb{C}^g \times \mathbb{C}^g \to \mathbb{R}$ 是一个双线性反对称型, $E : \Lambda \times \Lambda \to \mathbb{Z}$ 且满足:

$$E(ix, iy) = E(x, y).$$

命题 3.12　厄密特形式与反对称形式的黎曼型集合存在一一对应：

$$H \mapsto \mathrm{Im}(H), \quad E \mapsto E(ix, y) + iE(x, y).$$

证明　可以参考 [50] 引理 A 5.0.2. □

通过 θ 级数的理论可以得到, $\mathbb{C}^g/\Lambda$ 上有强的线丛或者可以嵌入射影空间当且仅当其上有非退化的黎曼型 (这时称其是极化的).

命题 3.13　对于 $\phi : \mathbb{C}^g/\Lambda \hookrightarrow \mathbb{P}^n$, 存在一组 Frobenius 基, 使得

$$\Lambda = \mathbb{Z}e_1 + \cdots + \mathbb{Z}e_g + \mathbb{Z}f_1 + \cdots + \mathbb{Z}f_g,$$

满足条件

$$E(e_i, e_j) = E(f_i, f_j) = 0, \quad E(e_i, f_j) = \begin{cases} d_i, & i = j, \\ 0, & i \neq j, \end{cases}$$

其中 $d_1 \mid d_2 \mid \cdots d_g$.

证明　可以参考 [50] 引理 A 5.3.1. □

定义 3.17　定义

$$\det(E) = (d_1 \cdots d_g)^2,$$

如果 $\det(E) = 1$, 则称其为主极化的.

3.4.2　复数域上的雅可比簇

定义 3.18　曲线 C 的雅可比簇是：

$$\mathrm{Jac}(C) = H^0(X, \Omega_X)^* \big/ H_1(X, \mathbb{Z}).$$

记

$$H^0(X,\Omega_X)^* = \langle \omega_1, \cdots, \omega_g \rangle,\ \ H_1(X,\mathbb{Z}) = \langle \gamma_1, \cdots, \gamma_{2g} \rangle,$$

$$\Omega_1 = \begin{pmatrix} \int_{\gamma_1}\omega_1 & \cdots & \int_{\gamma_g}\omega_1 \\ \cdots & \cdots & \cdots \\ \int_{\gamma_1}\omega_g & \cdots & \int_{\gamma_g}\omega_g \end{pmatrix}, \quad \Omega_2 = \begin{pmatrix} \int_{\gamma_{g+1}}\omega_1 & \cdots & \int_{\gamma_{2g}}\omega_1 \\ \cdots & \cdots & \cdots \\ \int_{\gamma_{g+1}}\omega_g & \cdots & \int_{\gamma_{2g}}\omega_g \end{pmatrix}.$$

定义 3.19　作为复环面, 雅可比簇可以定义为：

$$\mathbb{C}^g/\Lambda,$$

其中

$$\Lambda = \mathbb{Z}^g + \Omega_1^{-1}\Omega_2\mathbb{Z}^g,$$

可以证明其为射影簇, 且有黎曼型, 即亏格为 g 的超椭圆曲线的雅可比簇是 g 维阿贝尔簇.

定义 3.20　固定一个基点 $a \in X$, 雅可比嵌入为

$$\Phi_a : X \to \mathrm{Jac}(X) = \mathbb{C}^g/\Lambda,\ \ b \to \Big(\int_a^b \omega_1, \cdots, \int_a^b \omega_g\Big) \mod \Lambda.$$

可以看出与 a 的取值无关, 从而可以定义:

$$\Phi : \mathrm{Div}^0(X) \to \mathrm{Jac}(X);\ \sum n_i(b_i) \to \sum n_i\Phi_a(b_i).$$

定理 3.14　(阿贝尔-雅可比定理) 映射 $\Phi : \mathrm{Div}^0(X) \to \mathrm{Jac}(X)$ 是满射, 且其核为主除子组成的子群. 即有:

$$\mathrm{Pic}^0(X) \cong \mathrm{Jac}(X).$$

证明　证明参考 [50] 定理 A.6.3.2.　□

3.5　阿贝尔簇和同源

从代数几何的角度:

定义 3.21　阿贝尔簇是完备的连通的群簇. 在其上可以定义加法和逆运算并且满足交换性.

定理 3.15　设 $\alpha : A \to B$ 为阿贝尔簇上的同态. 则以下条件等价：

(1) α 为满射且 $\ker(\alpha)$ 的维数为 0;

(2) α 为满射且 $\dim(A) = \dim(B)$;

(3) $\ker(\alpha)$ 的维数为 0 且 $\dim(A) = \dim(B)$.

证明　证明参考 [53] 性质 8.1. □

定义 3.22　称上面定理的同态 α 为同源, 它的次数定义为 $\deg(\alpha) = [\overline{K}(A) : \alpha^*\overline{K}(B)]$.

3.5.1　极化阿贝尔簇

定义 3.23　对于给定的可逆层 $\mathscr{L}$, 定义:

$$\lambda_{\mathscr{L}} : A \to \mathrm{Pic}(A);\ a \to {t_a}^*\mathscr{L} \otimes \mathscr{L}^{-1},$$

其中

$$t_a : A \to A;\ b \to a + b$$

为平移映射.

阿贝尔簇

$$\hat{A} = \mathrm{Pic}^0(A) = \{\mathscr{L} \mid {t_a}^*\mathscr{L} \cong \mathscr{L}\ \forall a \in A\},$$

称为 A 的对偶.

定理 3.16　对于 $\lambda_{\mathscr{L}} : A \to \mathrm{Pic}(A);\ a \to {t_a}^*\mathscr{L} \otimes \mathscr{L}^{-1}$,

(1) $\lambda_{\mathscr{L}}$ 的像在 $\mathrm{Pic}^0(A)$ 中.

(2) 如果 $\mathscr{L}^{\otimes n} \in \mathrm{Pic}^0(A)(n \neq 0)$, 则 $\mathscr{L} \in \mathrm{Pic}^0(A)$.

(3) 当 $\mathscr{L}$ 是强的, 则有 $\{{t_a}^*\mathscr{L} \cong \mathscr{L}\ \forall a \in A\}$ 的维数是 0. 即有 $\lambda_{\mathscr{L}} : A \to \mathrm{Pic}^0(A)$ 是一个同源.

证明　证明参考 [53]13 节. □

定义 3.24　若 $\lambda_{\mathscr{L}} : A \to \mathrm{Pic}^0(A)$ 是同源, 称 $\mathscr{L}$ 为极化 (由可逆层和除子一一对应也可以称 $\mathscr{L}$ 对应的除子 P 为极化除子), 此时称 (A, P) 为极化阿贝尔簇.

若还有 $\lambda_{\mathscr{L}}$ 是同构, 即 $\deg(\lambda_{\mathscr{L}}) = 1$, 则称 $\mathscr{L}$ 为主极化 (即 P 为主极化除子), 此时称 (A, P) 为极化阿贝尔簇.

我们主要考虑的是主极化的阿贝尔簇, 即 $A \cong \hat{A}$. 之后我们考虑主极化阿贝尔簇时, 可以记为 $\mathcal{A} = (A, P)$, 其中 P 为对应的主极化除子.

定理 3.17　设 $\alpha : A \to B$ 为主极化阿贝尔簇的同源, 则存在唯一的同源 $\hat{\alpha} : B \to A$, 使得:

$$\alpha\hat{\alpha} = [\deg(\alpha)],\ \ \hat{\alpha}\alpha = [\deg(\alpha)].$$

这里 $[m]$ 表示倍乘运算.

证明　可以参考 [54] 命题 5.12. □

3.5.2　韦伊配对

这里可以参考 [53] 第 16 节.

对于 $a \in A[m]$, $a' \in \hat{A}[m]$, 设 a' 对应除子 D, 则

$$m^* D \sim mD \sim 0.$$

设 $mD = (f)$, $m^* D = (g)$, 则有:

$$(f \circ m) = m^*(f) = m(g) = (g^m),$$

从而,

$$g(x+a)^m = Cf \circ m(x+a) = Cf(mx+ma) = Cf(mx) = g(x)^m.$$

则

$$\frac{g(x+a)}{g(x)} \in \mu_m,$$

定义 3.25　韦伊配对即映射

$$e_m : A[m] \times \hat{A}[m] \to \mu_m;\ \ (a, a') \mapsto \frac{g(x+a)}{g(x)}.$$

它与 x 选择无关.

这里考虑主极化的阿贝尔簇, 即 $\lambda : A \cong \hat{A}$, 所以可以定义配对:

$$e_m^\lambda : A[m] \times A[m] \to \mu_m; \qquad (a, a') \mapsto e_m(a, \lambda(a')).$$

定义 3.26　对于 $A[m]$ 的子群 S, 如果 S 是极大的使得韦伊配对 $e_m|_{S\times S}$ 是平凡的, 则称 S 为极大 m-韦伊迷向子群.

定理 3.18　对于 $\mathcal{A} = (A, P)$ 为主极化的阿贝尔簇, S 为 $A[m]$ 的子群, 定义 $\phi : A \to A' = A/S$. 则存在 A' 上的主极化除子 P' 使得 $\phi^* P' \sim mP$ 当且仅当 S 为极大 m-韦伊迷向子群. 此时 $\mathcal{A}' = (A', P')$ 也为主极化阿贝尔簇.

证明　证明参考 [55]23 节定理 4, [56] 36 页.　□

为了方便我们之后用主极化除子代替主极化可逆层.

3.5.3　Rosati 对合

考虑阿贝尔簇 A, 其上极化 X 对应同源 $\lambda_X : A \to \hat{A}$, 此时 $\lambda^{-1} \in \mathrm{Hom}(\hat{A}, A) \bigotimes \mathbb{Q}$.

定义 3.27　设 $\alpha \in \mathrm{End}(A)$, 定义

$$\hat{\alpha} : \hat{A} \to \hat{A}; \qquad D \to \alpha^*(D).$$

定义 3.28　Rosati 对合：

$$\phi : \mathrm{End}(A) \bigotimes \mathbb{Q} \to \mathrm{End}(A) \bigotimes \mathbb{Q}; \qquad \alpha \to \alpha^{\dagger} = \lambda_X^{-1} \circ \hat{\alpha} \circ \lambda_X.$$

命题 3.19　映射

$$j : \mathrm{NS}(A) \bigotimes \mathbb{Q} \to \mathrm{End}(A) \bigotimes \mathbb{Q}; \qquad \bar{L} \to \lambda_X^{-1} \circ \lambda_L \tag{3.5}$$

的像在 Rosati 对合下不变.

证明　证明参见 [53] 命题 14.2. □

注　当 A 是主极化阿贝尔簇时, Rosati 对合是从 $\mathrm{End}(A)$ 到 $\mathrm{End}(A)$ 的映射且 j 是从 $\mathrm{NS}(A)$ 到 $\mathrm{End}(A)$ 的映射.

3.6　有限域上的阿贝尔簇

定理 3.20　(Hasse) 设 C 为有限域 $\mathbb{F}_q$ 上亏格为 g 的超椭圆曲线. 则

$$t = q + 1 - \#C(\mathbb{F}_q) \tag{3.6}$$

满足

$$| t | \leqslant 2g\sqrt{q}.$$

定理 3.21　(Tate) 设 A, B 为有限域 $\mathbb{F}_q$ 上的阿贝尔簇. 则存在定义在 $\mathbb{F}_q$ 上的同源 $\phi : A \to B$ 当且仅当 $\#A(\mathbb{F}_q) = \#B(\mathbb{F}_q)$.

证明　证明参考 [44]. □

3.6.1　正常和超奇异阿贝尔簇

对于有限域上维数为 g 的阿贝尔簇 A 的 m 阶挠点 $A[m] = \ker([m]) = \{P \in A(\overline{K}) \mid mP = O\}$. 当 $p \nmid m$ 时, $A[m] \cong (\mathbb{Z}/m\mathbb{Z})^{2g}$. 对于 $r \geqslant 1$, 则 $A[p^r] \cong (\mathbb{Z}/m\mathbb{Z})^t$ (其中 $0 \leqslant t \leqslant g$).

定义 3.29　若 $A[p^r]$ 的秩为 g, 则称其为正常的 (ordinary); 若 A 可以同源到两条超奇异椭圆曲线的乘积, 则称其为超奇异的 (supersingular).

命题 3.22　在维数是 2 的情形, 当 $A[p^r]$ 的秩是 0 时, A 是超奇异的.

3.6.2　超奇异阿贝尔簇和超特殊阿贝尔簇

这部分可以参考 [57].

定义 3.30　超奇异阿贝尔簇 A 是可以同源到超奇异椭圆曲线的乘积 $E_1 \times E_2 \cdots \times E_g$ 的阿贝尔簇. 超特殊阿贝尔簇 A 是可以同构到超奇异椭圆曲线的乘积 $E_1 \times E_2 \cdots \times E_g$ 的阿贝尔簇.

作为簇这与超奇异椭圆曲线的取法无关, 只有一个同构类 E^g, 但是不同超奇异椭圆曲线乘积对应的主极化除子是不同的, $E_1 \times E_2 \cdots \times E_g$ 对应的主极化除子是 $\{0\} \times E_2 \cdots \times E_g + \cdots + E_1 \times E_2 \cdots \times E_{g-1} \times \{0\}$.

超奇异阿贝尔簇的模空间维数是 $[\frac{g^2}{4}]$, 而超特殊阿贝尔簇的模空间维数是 0. 所以在密码学应用中会选择超特殊阿贝尔簇作为研究对象.

3.7　阿贝尔曲面

由于主要研究维数是 2 的阿贝尔簇, 这是一个代数曲面, 也称为阿贝尔曲面. 所以需要一些代数曲面的知识.

3.7.1　代数曲面上的除子

由于除子是余维数是 1 的正则概型, 所以曲面上的除子是曲线.

定义 3.31　设代数曲面 X 上的两条不同的不可约曲线 C, C'. 对于 $x \in C \cap C'$, 设 f, g 为 C, C' 在 x 处的方程, C, C' 在 x 处的相交数是

$$\mathrm{mult}_x(C, C') = \dim_{\mathbb{C}}(\mathcal{O}_{X,x} \big/ \langle f, g \rangle),$$

C, C' 的相交数是

$$C \bullet C' = \sum_{x \in C \cap C'} \mathrm{mult}_x(C, C').$$

定义 3.32　对于线丛 (可逆层)$\mathscr{L}$, 定义示性数为:

$$\chi(\mathscr{L}) = \dim(H^0(X, \mathscr{L})) - \dim(H^1(X, \mathscr{L})) + \dim(H^2(X, \mathscr{L})).$$

定义 3.33　对于线丛 (可逆层)$\mathscr{L}, \mathscr{M}$, 定义其相交数为:

$$\mathscr{L} \bullet \mathscr{M} = \chi(\mathcal{O}_X) - \chi(\mathscr{L}^{-1}) - \chi(\mathscr{M}^{-1}) + \chi(\mathscr{L}^{-1} \bigotimes \mathscr{M}^{-1}).$$

定理 3.23　将除子 C 和线丛 (可逆层)$\mathcal{O}_X(C)$ 对应, 则

(1) $\mathcal{O}_X(C) \bullet \mathcal{O}_X(C') = C \bullet C'$.

(2) 当 C 光滑时, $\mathcal{O}_X(C) \bullet \mathscr{L} = \deg(\mathscr{L} \mid_C)$.

证明　证明参考 [58] 引理 2.4.1, 2.4.2. □

从而可以定义双线性型:

$$F : \mathrm{Pic}(X) \times \mathrm{Pic}(X) \to \mathbb{Z}; (C, C') \mapsto C \bullet C'.$$

3.7.2　代数曲面上的黎曼-洛赫定理

定理 3.24　(黎曼-洛赫定理) 设于 X 是光滑的射影曲面. 对于 $\mathscr{L} \in \mathrm{Pic}(X)$ 有

$$\chi(\mathscr{L}) = \chi(\mathcal{O}_X) + \frac{1}{2}(\mathscr{L}^2 - \mathscr{L} \bullet \mathcal{O}_X(K_X)), \tag{3.7}$$

其中 K_X 为由微分定义的正则除子.

证明　证明参考 [58] 定理 2.4.5. □

3.7.3　阿贝尔曲面

对于阿贝尔曲面, 有结果:

$$K_X = 0,\ \chi(\mathcal{O}_X) = 0,\ p_g = \dim(H^2(X, \mathcal{O}_X)) = 1,\ q = \dim(H^1(X, \mathcal{O}_X)) = 2.$$

当 $\mathscr{L}$ 强时, $\dim(H^2(X, \mathscr{L})) = \dim(H^1(X, \mathscr{L})) = 0$. 由黎曼-洛赫定理计算可得：

$$\chi(\mathscr{L}) = \dim(H^0(X, \mathscr{L})) = \frac{1}{2}\mathscr{L}^2.$$

又由于 $\chi(\mathscr{L})^2 = \deg(\phi_{\mathscr{L}})$, 综上有：

$$(\mathscr{L} \bullet \mathscr{L})^2 = 4\deg(\phi_{\mathscr{L}}).$$

3.7.4　除子等价与 NS 群

定义 3.34　(1) 除子等价：如果 X 上的两个除子 D, D' 之间相差一个主除子, 则称 D, D' 等价, 记为 $D \sim D'$.

(2) 除子数值等价: 如果两个除子 D, D' 满足 $(D - D') \bullet C = 0$(对于任意 X 上的不可约曲线 C), 则称 D, D' 数值等价, 记为 $D \approx D'$.

(3) NS 群 (Neron-Severi 群)：$\mathrm{NS}(X) = \mathrm{Pic}(X)/\mathrm{Pic}^0(X)$.

定理 3.25　(1) 除子 D 数值等价于 0 当且仅当 $mD \in \mathrm{Pic}^0(X)$, 即 $D \in \mathrm{Tor}(\mathrm{Pic}(X)/\mathrm{Pic}^0(X))$.

(2) 对于阿贝尔簇 A, 定义 ϕ : $\mathrm{NS}(A) \to \mathrm{Hom}(A, \hat{A})$; $\overline{\mathscr{L}} \to \lambda_{\mathscr{L}}$ 为一个单射, 从而 $\mathrm{NS}(A)$ 是一个自由 $\mathbb{Z}$ 模, 且秩是 $\leqslant 4\dim(A)^2$.

(3) 在阿贝尔簇的条件下, $\mathrm{NS}(A)$ 自由, 则 D, D' 数值等价当且仅当 D, D' 在 $\mathrm{NS}(A)$ 中相同.

证明　证明参考 [53] 推论 10.18, [58] 定理 2.5.3. □

第 4 章　同源图及其性质

4.1　图的基础知识

定义 4.1

(1) 记一个图为 $\mathcal{G}$, 其顶点集合记为 V, 边为连接两个顶点的路径.

(2) 顶点 v 的输出次数为从 v 出发的边的个数, 顶点 v 的输入次数为进入 v 的边的个数.

(3) 从顶点 v 到自己的边称为一条环路, 和 v 通过一条边相连的顶点称为 v 的邻接.

(4) (无向图) 若每个顶点输出次数和输入次数相同, 则称其为无向图.

(5) (正则图) 若无向图每个顶点的次数均为 d, 则称为 d-正则图.

(6) (连通图) 若任意两个顶点都可以找到路径连接, 则称这个图为连通图.

(7) (拉马努金图) 若一个图是 n 个顶点的连通图的 d-正则图, 且对于特征值 λ_i, $\max\{|\lambda_i| : \lambda_i \neq d\} \leqslant 2\sqrt{d-1}$, 则称这个图为拉马努金图.

4.2　椭圆曲线同源图

我们考虑的域 K 是 $\overline{\mathbb{F}}_p$ 的子域 ($p \neq 2, 3$), $\ell \neq p$ 是另一个素数.

定义 4.2　定义 K 上的超奇异椭圆曲线同源图为 $\mathcal{G}_\ell(K)$, 其中顶点 $V(K)$ 为所有 K 上的超奇异椭圆曲线的 K-同构类, 将 E 的 K 同构类记为 $[E]$, 边为两个顶点之间的 ℓ-同源等价类. 这里当图中的顶点 $[E_1] = [E_1']$, $[E_2] = [E_2']$, $\phi : E_1 \to E_2$, $\phi' : E_1' \to E_2'$ 为两个次数是 ℓ 的 K-同源, 如果存在同构 $\tau_1 : E_1 \to E_1'$, $\tau_2 : E_2 \to E_2'$, 使得 $\phi' \circ \tau_1 = \tau_2 \circ \phi$, 则称 ϕ, ϕ' 是等价的同源.

定义 4.3　若 $\phi : E_1 \to E_2$ 满足 $\pi(\ker\phi) = \ker\phi$, 其中 π 是 $\mathbb{F}_{p^2}$(或 $\mathbb{F}_p$) 上的 Frobenius 映射, 则称 ϕ 是定义在 $\mathbb{F}_{p^2}$(或 $\mathbb{F}_p$) 上的同源.

由定理 2.20 (3) 知, 超奇异椭圆曲线都可以定义在 $\mathbb{F}_{p^2}$ 上, 我们只需要考虑 $\mathbb{F}_{p^2}$-图, $\mathbb{F}_p$-图和 $\overline{\mathbb{F}}_p$-图.

4.2.1　$\overline{\mathbb{F}}_p$-图 $\mathcal{G}_\ell(\overline{\mathbb{F}}_p)$

设 $K = \overline{\mathbb{F}}_p$. 则图 $\mathcal{G}_\ell(\overline{\mathbb{F}}_p)$ 的顶点集 $V_\ell(\overline{\mathbb{F}}_p)$ 是所有超奇异椭圆曲线的 j 不变量, 顶点数如下给出:

定理 4.1　记 $S_{p^2}(j)=\#V(\overline{\mathbb{F}}_p)$. 则

$$S_{p^2}(j)=\left[\frac{p}{12}\right]+\begin{cases}0, & p\equiv 1 \bmod 12,\\ 1, & p\equiv 5 \bmod 12,\\ 1, & p\equiv 7 \bmod 12,\\ 2, & p\equiv 11 \bmod 12.\end{cases} \tag{4.1}$$

此时多出的部分 $0,1,1,2$ 对应 $j=0,1728$ 是超奇异椭圆曲线的情况.

证明　可以参考 [40] 定理 4.1(c). □

图 $\mathcal{G}_\ell(\overline{\mathbb{F}}_p)$ 的边为所有 $\overline{\mathbb{F}}_p$ 上的 ℓ-同源. 由定理 2.18, $E[\ell]\cong(\mathbb{Z}/\ell\mathbb{Z})^2$ 有 $\ell+1$ 个 ℓ 阶子群, 从而每个点都恰好有 $\ell+1$ 条边.

根据命题 2.4, 当 $j\neq 1728,0$ 时, 椭圆曲线的自同构群是 $\{\pm 1\}$, 这样就得到它的输出边和输入边数相等. 从而当 $p\equiv 1 \bmod 12$ 时, 超奇异椭圆曲线同源 $\overline{\mathbb{F}}_p$-图是无向图. 又由 [34] 定理 13, 利用强逼近定理可知两条超奇异椭圆曲线可以通过 ℓ 的方幂次同源连接, 则超奇异椭圆曲线同源 $\overline{\mathbb{F}}_p$-图是连通图. 进一步由 [5] 知, 超奇异椭圆曲线同源 $\overline{\mathbb{F}}_p$-图是拉马努金图, 具有很好的混合性, 不易寻找同源, 因此可以在密码学中得到应用.

4.2.2　$\mathbb{F}_{p^2}$-图 $\mathcal{G}_\ell(\mathbb{F}_{p^2})$

由定理 2.22, 当 $p\neq 2,3$ 时, $\mathbb{F}_{p^2}$ 上的超奇异椭圆曲线的 Frobenius 映射的迹只能是 $0,\pm p$ 和 $\pm 2p$. 这时 j 不变量相同的超奇异椭圆曲线作为一个 $\overline{\mathbb{F}}_p$-同构类会分出不同的扭, 即分成不同的 $\mathbb{F}_{p^2}$-同构类.

记 $N(t)$ 为 $\mathbb{F}_q$ 上 Frobenius 映射的迹为 t 的椭圆曲线 $\mathbb{F}_q$ 同构类个数.

定理 4.2　当 $[\mathbb{F}_q:\mathbb{F}_p]$ 是偶数时,

$$N(t)=\begin{cases}\frac{1}{12}\cdot\left(p+6-4\left(\frac{-3}{p}\right)-3\left(\frac{-4}{p}\right)\right), & \text{若 } t^2=4q;\\ 1-\left(\frac{-3}{p}\right), & \text{若 } t^2=q;\\ 1-\left(\frac{-4}{p}\right), & \text{若 } t=0.\end{cases} \tag{4.2}$$

证明　可以参考 [45]. □

由于超奇异椭圆曲线的 j 不变量在 $\mathbb{F}_{p^2}$ 中, 需要考虑 $q=p^2$.

命题 4.3

(1) 当 $j=0$ 时, E_0 为 $\mathbb{F}_{p^2}$ 上的超奇异椭圆曲线当且仅当 $p\equiv 2 \bmod 3$. 此时, $E_0:y^2=x^3+1$ 在 $\mathbb{F}_{p^2}$ 上有六个扭, 即 $\mathbb{F}_{p^2}$ 同构类, 分别为

$$E_{0,\omega^i}:y^2=x^3+\omega^i\ (i\in\{0,1,2,3,4,5\}),$$

其中 ω 为 $\mathbb{F}_{p^2}^*/(\mathbb{F}_{p^2}^*)^6$ 的生成元, 且

(i) $\mathrm{tr}(E_{0,1}) = -2p$.

(ii) $\mathrm{tr}(E_{0,\omega}) = -p$.

(iii) $\mathrm{tr}(E_{0,\omega^2}) = p$.

(iv) $\mathrm{tr}(E_{0,\omega^3}) = 2p$.

(v) $\mathrm{tr}(E_{0,\omega^4}) = p$.

(vi) $\mathrm{tr}(E_{0,\omega^5}) = -p$.

(2) 当 $j = 1728$ 时, E_{1728} 为 $\mathbb{F}_{p^2}$ 上的超奇异椭圆曲线当且仅当 $p \equiv 3 \bmod 4$. 此时, $E_{1728}: y^2 = x^3 + x$ 在 $\mathbb{F}_{p^2}$ 上有四个扭, 即 $\mathbb{F}_{p^2}$ 同构类, 分别为

$$E_{1728,\omega^i}: y^2 = x^3 + \omega^i x \ (i \in \{0,1,2,3\}),$$

其中 ω 为 $\mathbb{F}_{p^2}^*/(\mathbb{F}_{p^2}^*)^4$ 生成元, 且

(i) $\mathrm{tr}(E_{1728,1}) = -2p$.

(ii) $\mathrm{tr}(E_{1728,\omega}) = 0$.

(iii) $\mathrm{tr}(E_{1728,\omega^2}) = 2p$.

(iv) $\mathrm{tr}(E_{1728,\omega^3}) = 0$.

证明　参考 [21], [40] 第十章命题 5.4 , 推论 5.4.1. □

注　这个定理说明当 $p \equiv 2 \bmod 3$ 时, $j = 0$ 的超奇异椭圆曲线类中有两个 $\mathbb{F}_{p^2}$ 上的同构类的迹是 p, 另外两个是 $-p$. 当 $p \equiv 3 \bmod 4$ 时, $j = 1728$ 的超奇异椭圆曲线类中有两个 $\mathbb{F}_{p^2}$ 上的同构类的迹是 0. 由此 $N(t)$ 中同构类的迹是 p 和 $-p$ 对应 $j = 0$ 椭圆曲线, $N(t)$ 中同构类的迹是 0 对应 $j = 1728$ 的椭圆曲线.

不变量 $j = 0$ 或 $j = 1728$ 的超奇异椭圆曲线类中都恰好有一个同构类的迹为 $2p$ 或 $-2p$. 对于 $j \neq 0, 1728$ 时, 只有两个扭. 从而 $j \neq 0, 1728$ 对应的迹为 $2p$ 或 $-2p$. 所有 j 不变量和 F_{p^2} 上的迹是 $2p$ 或 $-2p$ 的同构类是一一对应的.

记 $\mathcal{G}_\ell(\mathbb{F}_{p^2}, t)$ 为迹为 t 的顶点构成的 $\mathcal{G}_\ell(\mathbb{F}_{p^2})$-子图, 这是由定理 2.1(Tate 定理), 只有迹相同的时候才有同源可以连接.

定理 4.4　对于子图 $\mathcal{G}_\ell(\mathbb{F}_{p^2}, 0)$, $\mathcal{G}_\ell(\mathbb{F}_{p^2}, \pm p)$ 和 $\mathcal{G}_\ell(\mathbb{F}_{p^2}, \pm 2p)$, 有如下结果:

(1) 当 $p \equiv 3 \bmod 4$, $\mathcal{G}_\ell(\mathbb{F}_{p^2}, 0)$ 有两个顶点，j 不变量均是 1728, 且

(i) $\mathcal{G}_2(\mathbb{F}_{p^2}, 0)$ 每个顶点有一条环路.

(ii) 当 $\ell \equiv 3 \bmod 4$ 时, $\mathcal{G}_\ell(\mathbb{F}_{p^2}, 0)$ 顶点都没有边.

(iii) 当 $\ell \equiv 1 \bmod 4$ 时, $\mathcal{G}_\ell(\mathbb{F}_{p^2}, 0)$ 每个顶点有两条环路.

(2) 当 $p \equiv 2 \bmod 3$ 时, $\mathcal{G}_\ell(\mathbb{F}_{p^2}, \pm p)$ 各有两个顶点，j 不变量均是 0, 且

(i) $\mathcal{G}_3(\mathbb{F}_{p^2}, \pm p)$ 每个顶点有一条环路.

(ii) 当 $\ell \equiv 2 \bmod 3$ 时, $\mathcal{G}_\ell(\mathbb{F}_{p^2}, \pm p)$ 顶点都没有边.

(iii) 当 $\ell \equiv 1 \bmod 3$ 时, $\mathcal{G}_\ell(\mathbb{F}_{p^2}, \pm p)$ 每个顶点有两条环路.

(3) $\mathcal{G}_\ell(\mathbb{F}_{p^2}, \pm 2p) \cong \mathcal{G}_\ell(\overline{\mathbb{F}_p})$.

证明　证明参考 [21] 定理 3, 定理 4, 定理 5, 定理 6. □

所以研究 $\mathbb{F}_{p^2}$-子图 $\mathcal{G}_\ell(\mathbb{F}_{p^2}, \pm 2p)$ 和研究 $\overline{\mathbb{F}_p}$-图是一致的.

4.2.3　$\mathbb{F}_p$-图 $\mathcal{G}_\ell(\mathbb{F}_p)$

我们首先给出一个判断超奇异椭圆曲线定义在 $\mathbb{F}_p$ 上的方法：

定理 4.5　对于 $p > 3$, E 是 $\overline{\mathbb{F}}_p$ 上的超奇异椭圆曲线, 则 E 定义在 $\mathbb{F}_p$ 上当且仅当 $\mathbb{Z}[\sqrt{-p}] \subseteq \mathrm{End}(E)$.

证明　证明参考 [11] 性质 2.4. □

当考虑 $\mathbb{F}_p$ 图时 ($p > 3$), 此时顶点集 $V_\ell(\mathbb{F}_p)$ 为所有落在 $\mathbb{F}_p$ 中的超奇异椭圆曲线的 j 不变量,

定理 4.6　记 $S_p(j) = \#V(\mathbb{F}_p)$. 则

$$S_p(j) = \begin{cases} \frac{1}{2}h(-p), & p \equiv 1 \bmod 4, \\ 2h(-p), & p \equiv 3 \bmod 8, \\ h(-p), & p \equiv 7 \bmod 8, \end{cases} \tag{4.3}$$

这里 $h(-p)$ 是虚二次域 $\mathbb{Q}(\sqrt{-p})$ 的类数.

设 E 是定义在 $\mathbb{F}_p$ 上的超奇异椭圆曲线, 我们知道 $\pi \in \mathrm{End}_{\mathbb{F}_p}(E)$, 但是此时由 (2.10) 和迹为 0 可知 $\pi^2 + p = 0$, 从而 $\mathrm{End}_{\mathbb{F}_p}(E)$ 为虚二次域 $K = \mathbb{Q}(\sqrt{-p})$ 的序. 更进一步地, 由 $\mathbb{Z}[\pi] = \mathbb{Z}[\sqrt{-p}] \subseteq \mathrm{End}_{\mathbb{F}_p}(E) \subseteq \mathcal{O}_K$. 此时有以下两种情况：

(1) 当 $p \equiv 1 \bmod 4$ 时, $d_K = -4p$, $\mathcal{O}_K = \mathbb{Z}[\pi]$. 则 $\mathrm{End}(E) = \mathbb{Z}[\pi]$.

(2) 当 $p \equiv 3 \bmod 4$ 时, $d_K = -p$, $\mathcal{O}_K = \mathbb{Z}[\frac{1+\pi}{2}]$.

故 $\mathrm{End}(E)$ 为 $\mathbb{Z}[\pi]$ 或者 $\mathbb{Z}[\frac{1+\pi}{2}]$.

定义 4.4　设 $\mathcal{O}$ 等于 $\mathbb{Z}[\pi]$ 或者 $\mathbb{Z}[\frac{1+\pi}{2}]$ 是虚二次域 $K = \mathbb{Q}(\sqrt{-p})$ 的序. 记 $\mathrm{Ell}_{\mathcal{O}}(\mathbb{F}_p) = \{E \mid E$ 为定义在 $\mathbb{F}_p$ 上的超奇异椭圆曲线且 $\mathrm{End}_{\mathbb{F}_p}(E) = \mathcal{O}\}$.

下面这个定理在构造 CSIDH 密码协议中起到关键作用:

定理 4.7　理想类群 $\mathrm{Cl}(\mathcal{O})$ 在 $\mathrm{Ell}_{\mathcal{O}}(\mathbb{F}_p)$ 上的作用

$$\mathrm{Cl}(\mathcal{O}) \times \mathrm{Ell}_{\mathcal{O}}(\mathbb{F}_p) \to \mathrm{Ell}_{\mathcal{O}}(\mathbb{F}_p); \ ([I], E) \mapsto IE = E/E[I]$$

是自由和传递的.

证明　证明参考 [42] 推论 23.8. □

定义 4.5　设 E 是 $\mathbb{F}_p$ 上的超奇异椭圆曲线.

(1) 若 $\mathrm{End}_{\mathbb{F}_p}(E)=\mathcal{O}_K$, 则称 E 在顶面上.

(2) 若 $\mathrm{End}_{\mathbb{F}_p}(E)=\mathbb{Z}[\pi]$, 则称 E 在底面上.

定义 4.6　当 $p\equiv 3 \bmod 4$ 时, 对于定义在 $\mathbb{F}_p$ 上的超奇异椭圆曲线 E_1, E_2 和同源 $\phi: E_1\to E_2$,

(1) 若 $\mathrm{End}_{\mathbb{F}_p}(E_1)=\mathrm{End}_{\mathbb{F}_p}(E_2)$, 则称 ϕ 水平;

(2) 若 E_1 在顶面上, E_2 在底面上, 则称 ϕ 下降;

(3) 若 E_1 在底面上, E_2 在顶面上, 则称 ϕ 上升.

引理 4.8　设 $\phi: E_1\to E_2$ 为 ℓ 次同源, 若 ϕ 为非水平的 $\mathbb{F}_p$ 同源, 则 $\ell=2$ (此时不考虑同构).

证明　证明参考 [11] 引理 2.2.　□

与复数域上的椭圆曲线类似, 在有限域 $\mathbb{F}_p$ 上的椭圆曲线的 ℓ 同源也有水平上升下降的关系, 由引理可以看出 $\ell\neq 2$ 时只有水平的同源, 此时有结果：

定理 4.9　设 p 为一个素数, $p>3$, 在 $\mathcal{G}_\ell(\mathbb{F}_p)$ 图上有：

1. 当 $p\equiv 1 \bmod 4$ 时, 有 $h(-4p)$ 个超奇异椭圆曲线 $\mathbb{F}_p$ 同构类, 自同态环都为 $\mathbb{Z}[\sqrt{-p}]$, 此时每一个顶点都有两个 $\mathbb{F}_p$ 上的 2-同源, 且当 $\ell>2$, $(\frac{-p}{\ell})=1$ 时, 每个点有两个 $\mathbb{F}_p$ 上的 ℓ-同源.
2. 当 $p\equiv 7 \bmod 8$ 时, 有 $h(-p)$ 个超奇异椭圆曲线 $\mathbb{F}_p$ 同构类在顶面上, 也有 $h(-p)$ 个超奇异椭圆曲线 $\mathbb{F}_p$ 同构类在底面上, 此时顶面和底面的点一对一通过 2-同源相连, 且每个顶面的点通过两个 2-同源连接其他顶面的点. 且当 $\ell>2$, $(\frac{-p}{\ell})=1$ 时, 每个点有两个 $\mathbb{F}_p$ 上的 ℓ-同源.
3. 当 $p\equiv 3 \bmod 8$ 时, 有 $h(-p)$ 个超奇异椭圆曲线 $\mathbb{F}_p$ 同构类在顶面上, 也有 $3h(-p)$ 个超奇异椭圆曲线 $\mathbb{F}_p$ 同构类在底面上, 此时顶面和底面的点一对三通过 2-同源相连, 此时没有水平的 2-同源. 且当 $\ell>2$, $(\frac{-p}{\ell})=1$ 时, 每个点有两个 $\mathbb{F}_p$ 上的 ℓ-同源.

证明　证明参考 [11] 定理 2.7.　□

4.3　阿贝尔簇同源图

在本节我们考虑有限域上的二维主极化阿贝尔簇. 同上节一样, 我们考虑的域是 $\overline{\mathbb{F}}_p$ 的子域 ($p\neq 2,3$), $\ell\neq p$ 是另一个素数.

4.3.1　超奇异主极化阿贝尔簇同源图

$\overline{\mathbb{F}}_p$ 上的二维超奇异主极化阿贝尔簇有两种形式：

(1) 超椭圆曲线的雅可比簇 $\mathrm{Jac}(C)$, 其中 C 是亏格为 2 的超椭圆曲线.

(2) $E_1 \times E_2$, 其中 E_1, E_2 为超奇异椭圆曲线.

定义 4.7　超奇异主极化阿贝尔簇同源图 $\mathcal{G}'_{p,\ell}$ 的顶点是二维超奇异主极化阿贝尔簇 $\overline{\mathbb{F}}_p$ 同构类, 边是 (ℓ,ℓ)-同源等价类, 其中两条 (ℓ,ℓ)-同源等价是指它们有相同的核.

由定理 3.18, 只有当选择极大 n-韦伊迷向子群作为核时, 才有从超奇异主极化阿贝尔簇到超奇异主极化阿贝尔簇的同源, 从而极大 ℓ-韦伊迷向子群对应着 (ℓ,ℓ) 同源的个数.

定理 4.10　对于二维超奇异主极化阿贝尔簇 A, $A[\ell^n]$ 的 ℓ^n-韦伊迷向子群有如下形式：

(1) $\mathbb{Z}/\ell^n\mathbb{Z} \times \mathbb{Z}/\ell^n\mathbb{Z}$;

(2) $\mathbb{Z}/\ell^n\mathbb{Z} \times \mathbb{Z}/\ell^{n-k}\mathbb{Z} \times \mathbb{Z}/\ell^k\mathbb{Z}$ (其中 $0 \leqslant k \leqslant [\frac{n}{2}]$).

定理 4.11　对于二维超奇异主极化阿贝尔簇 A, $A[\ell^n]$ 的 ℓ^n-韦伊迷向子群 $(n > 2)$ 的个数为：

(1) $\ell^{2n-3}(\ell^2+1)(\ell+1)(\ell^n + \ell\frac{\ell^{n-2}-1}{\ell-1} + 1)$, 若 n 为偶数;

(2) $\ell^{2n-3}(\ell^2+1)(\ell+1)(\ell^n + \frac{\ell^{n-1}-1}{\ell-1})$, 若 n 为奇数.

证明　证明参见 [31].　□

4.3.2　超特殊阿贝尔簇 Richelot 同源图

$\overline{\mathbb{F}}_p$ 上二维主极化超特殊阿贝尔簇有两种形式：

(1) 超椭圆曲线的雅可比簇 Jac(C), 其中 C 是亏格为 2 的超椭圆曲线, 此时称 C 为超特殊曲线.

(2) $E_1 \times E_2$, 其中 E_1, E_2 为椭圆曲线.

1. Richelot 同源图的定义

定义 4.8　若 A_1, A_2 为定义在 $\overline{\mathbb{F}}_p$ 上的二维超特殊主极化阿贝尔簇, 同源 $\phi: A_1 \to A_2$ 满足 $\ker(\phi) = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, 则称其为 $(2,2)$-同源, 也称为 Richelot 同源. 此时存在 $\hat{\phi} \circ \phi = [2]$.

定义 4.9　超特殊 Richelot 同源图 $\mathcal{G}_{p,2}$ 的顶点集由所有的 2 维超特殊主极化阿贝尔簇 $\overline{\mathbb{F}}_p$ 同构类组成, 对于图中的两点 $[A_1], [A_2]$, 连接 $[A_1]$ 到 $[A_2]$ 之间的一条边是指一个 Richelot 同源的等价类, 这里两个 Richelot 同源等价是指它们有相同的核.

记超特殊阿贝尔簇 Richelot 同源图为 $\mathcal{G}_p$, $V(\mathcal{G}_p)$ 为顶点集合, $\mathcal{E}_p$ 为两条椭圆曲线乘积的顶点集合, $\mathcal{J}_p$ 为超椭圆曲线雅可比簇的顶点集合, 则 $V(\mathcal{G}_p) = \mathcal{E}_p \cup \mathcal{J}_p$.

命题 4.12　考虑图 $\mathcal{G}_p$.

(1) 它的顶点个数如下给出:

(i) 当 $p=2,3$ 时,

$$\#\mathcal{J}_p=0,\qquad \#\mathcal{E}_p=1.$$

(ii) 当 $p=5$ 时,

$$\#\mathcal{J}_p=1,\qquad \#\mathcal{E}_p=1.$$

(iii) 当 $p>5$ 时,

$$\#\mathcal{J}_p=\frac{p^3+24p^2+141p-346}{2880},\qquad \#\mathcal{E}_p=\frac{1}{2}S_{p^2}(j)(S_{p^2}(j)+1),$$

(其中 $S_{p^2}(j)$ 为超奇异椭圆曲线同构类的个数).

(2) 每个顶点的极大 2-韦伊迷向子群的个数是 $(2+1)(2^2+1)=15$. 从而输出边的个数是 15.

证明　参考 [32] 定理 2. □

2. Richelot 同源图边的计算: 雅可比簇形式

由 [32], 在 Jac(C) 中,

$$C:\ y^2=\prod_{i=1}^{6}(x-\alpha_i). \tag{4.4}$$

记

$$y^2=G_1G_2G_3, \tag{4.5}$$

其中

$$G_1=(x-\alpha_1)(x-\alpha_2)=g_{1,3}x^2+g_{1,2}x+g_{1,1}. \tag{4.6}$$

$$G_2=(x-\alpha_3)(x-\alpha_4)=g_{2,3}x^2+g_{2,2}x+g_{2,1}. \tag{4.7}$$

$$G_3=(x-\alpha_5)(x-\alpha_6)=g_{3,3}x^2+g_{3,2}x+g_{3,1}. \tag{4.8}$$

Jac(C) 二阶点为:

$$(\alpha_i,0)-(\alpha_j,0)(i<j).$$

则极大 2-韦伊迷向子群有形式:

$$S=\{0,[(\alpha_{i(1)}-\alpha_{i(2)})],[(\alpha_{i(3)}-\alpha_{i(4)})],[(\alpha_{i(5)}-\alpha_{i(6)})]\}, \tag{4.9}$$

其中 $\{i(1),\cdots,i(6)\}=\{1,2,3,4,5,6\}$, 且 $i(1)<i(2), i(3)<i(4), i(5)<i(6)$.

下面的定理说明 S 对应的同源:

定理 4.13　设超椭圆曲线 C 方程为 (4.5), S 为极大 2-韦伊迷向子群有形式 (4.9), 令

$$\phi:\ \mathrm{Jac}(C)\to A\cong \mathrm{Jac}(C)/S$$

为 S 决定的 $(2,2)$ 同源 (Richelot 同源). 令

$$\delta = \det \begin{pmatrix} g_{1,3} & g_{1,2} & g_{1,1} \\ g_{2,3} & g_{2,2} & g_{2,1} \\ g_{3,3} & g_{3,2} & g_{3,1} \end{pmatrix}.$$

则有：

(1) 当 $\delta \neq 0$ 时, A 同构于一条超椭圆曲线的雅可比簇 $\mathrm{Jac}(C')$, 其中

$$C' : \ y^2 = \delta^{-1} H_1(x) H_2(x) H_3(x) \tag{4.10}$$

$$H_1 = G_2' G_3 - G_2 G_3', H_2 = G_3' G_1 - G_3 G_1', H_3 = G_1' G_2 - G_1 G_2'. \tag{4.11}$$

此时

$$\phi : \mathrm{Jac}(C) \to \mathrm{Jac}(C') \cong \mathrm{Jac}(C)/S.$$

反之从 C' 出发, 对 H_1, H_2, H_3 做相同的计算则可以得到

$$\hat{\phi} : \mathrm{Jac}(C') \to \mathrm{Jac}(C).$$

(2) 当 $\delta = 0$ 时, 则 A 同构于两条超奇异椭圆曲线的乘积 $E_1 \times E_2$. 此时由 $\delta = 0$ 可以得到存在 $s_1, s_2 \in \mathbb{F}_{p^2}$ 使得

$$G_i = a_{i,1}(x - s_1)^2 + a_{i,2}(x - s_2)^2 \tag{4.12}$$

其中 $a_{i,1}, a_{i,2} \in \mathbb{F}_{p^2}$. 则记

$$E_1 : y^2 = \prod_{i=1}^{3} (a_{i,1} x + a_{i,2}), \tag{4.13}$$

$$E_2 : y^2 = \prod_{i=1}^{3} (a_{i,1} + a_{i,2} x). \tag{4.14}$$

从而 $\phi : C \to E_1 \times E_2$ 可以写成 $\phi_1 \times \phi_2$, 其中

$$\phi_1 : C \to E_1; (x, y) \to \left(\frac{(x - s_1)^2}{(x - s_2)^2}, \frac{y}{(x - s_2)^3}\right),$$

$$\phi_2 : C \to E_2; (x, y) \to \left(\frac{(x - s_2)^2}{(x - s_1)^2}, \frac{y}{(x - s_1)^3}\right).$$

证明　证明参考 [59]. □

3. Richelot 同源图边的计算: 椭圆曲线乘积形式

由 [32]: 在两条超奇异椭圆曲线的乘积 $E_1 \times E_2$ 中, 其中

$$E_1 : \ y^2 = \prod_{i=1}^{3}(x - \alpha_i), \tag{4.15}$$

$$E_2 : \ y^2 = \prod_{i=1}^{3}(x - \beta_i). \tag{4.16}$$

记

$$P_i = (\alpha_i, 0), \qquad Q_i = (\beta_i, 0). \tag{4.17}$$

则 15 个极大 2-韦伊迷向子群的形式为：

(i) 9 个是 $\{(\mathcal{O}_{E_1}, \mathcal{O}_{E_2}), (P_i, \mathcal{O}_{E_2}), (\mathcal{O}_{E_1}, Q_j), (P_i, Q_j)\}(i, j \in \{1, 2, 3\})$,

(ii) 6 个是 $\{(\mathcal{O}_{E_1}, \mathcal{O}_{E_2}), (P_1, Q_{\sigma(1)}), (P_2, Q_{\sigma(2)}), (P_3, Q_{\sigma(3)})\}(\sigma$ 置换 $\{1, 2, 3\})$.

定理 4.14　设 E_1 为对应方程 (4.15) 的超奇异椭圆曲线, E_2 为对应方程 (4.16) 的超奇异椭圆曲线. 记 P_i, Q_i 与 (4.17) 一致. 设

$$\phi : E_1 \times E_2 \to A \cong (E_1 \times E_2)/S$$

为 S 决定的 Richelot 同源.

(1) 选择核为 $\{(\mathcal{O}_{E_1}, \mathcal{O}_{E_2}), (P_i, \mathcal{O}_{E_2}), (\mathcal{O}_{E_1}, Q_j), (P_i, Q_j)\}$ 时, 则有 Richelot 同源是从椭圆曲线乘积到椭圆曲线乘积的同源, 即

$$A \cong E_1/\langle P_i \rangle \times E_2/\langle Q_j \rangle.$$

(2) 选择核为 $\{(\mathcal{O}_{E_1}, \mathcal{O}_{E_2}), (P_1, Q_{\sigma(1)}), (P_2, Q_{\sigma(2)}), (P_3, Q_{\sigma(3)})\}$ 时, 且 E_1 不同构 E_2 或者 E_1 同构于 E_2 但 $P_i \to Q_{\sigma(i)}$ 不可由 E_1 和 E_2 之间的同构诱导时, 则 A 同构于一条超椭圆曲线的雅可比簇 $\mathrm{Jac}(C_\sigma)$, 其中

$$C_\sigma : y^2 = -F_1(x)F_2(x)F_3(x) \tag{4.18}$$

$$F_i(x) = A(s_j - s_i)(s_i - s_k)x^2 + B(s'_j - s'_i)(s'_i - s'_k) \tag{4.19}$$

$$A = \frac{a_1}{a_2}\prod(s'_i - s'_j)^2, \qquad a_1 = \sum \frac{(s_j - s_i)^2}{s'_j - s'_i}, \qquad a_2 = \sum s_i(s'_k - s'_j) \tag{4.20}$$

$$B = \frac{b_1}{b_2}\prod(s_i - s_j)^2, \qquad b_1 = \sum \frac{(s'_j - s'_i)^2}{s_j - s_i}, \qquad b_2 = \sum s'_i(s_k - s_j) \tag{4.21}$$

(3) 选择核为 $\{(\mathcal{O}_{E_1}, \mathcal{O}_{E_2}), (P_1, Q_{\sigma(1)}), (P_2, Q_{\sigma(2)}), (P_3, Q_{\sigma(3)})\}$, 当 E_1 同构于 E_2 且 $P_i \to P_{\sigma(i)}$ 可由这个同构诱导时, 则 A 同构于两条椭圆曲线的乘积仍为 $E_1 \times E_2$.

证明　证明参考 [59]. □

4.3.3　Richelot 同源图已知结果

1. 约化自同构群的定义

定义 4.10　对于超椭圆曲线 C, 定义其约化自同构群为

$$\mathrm{RA}(C) = \mathrm{Aut}(C)\big/\langle \iota \rangle,$$

其中 ι 为超椭圆对合 (3.4).

定义 4.11　对 $\sigma \in \mathrm{RA}(C)$, 定义 $\tilde{\sigma} \in \mathrm{Aut}(C)$ 使得 $\tilde{\sigma} \bmod \langle \iota \rangle = \sigma$, 称 $\tilde{\sigma}$ 为 σ 的提升.

当 σ 为 $\mathrm{RA}(C)$ 中的二阶元时, 如果 $\tilde{\sigma}$ 为 $\mathrm{Aut}(C)$ 中的二阶元时, 称 σ 为长二阶元. 否则称其为短二阶元.

2. 约化自同构群的分类

由 [60], [51], 根据约化自同构群不同可以将超特殊曲线分为：

(1) $\mathrm{RA}(C) = 0$, 超特殊曲线个数

$$n_0 = \frac{(p-1)(p^2-35p+346)}{2880} - \frac{1-(\frac{-1}{p})}{32} - \frac{1-(\frac{-2}{p})}{8} - \frac{1-(\frac{-3}{p})}{9} + \begin{cases} 0, & p \equiv 1,2,3 \bmod 5, \\ -\frac{1}{5}, & p \equiv 4 \bmod 5. \end{cases}$$

(2) $\mathrm{RA}(C) = \mathbb{Z}/2\mathbb{Z}$, 超特殊曲线个数

$$n_1 = \frac{(p-1)(p-17)}{48} + \frac{1-(\frac{-1}{p})}{8} + \frac{1-(\frac{-2}{p})}{2} + \frac{1-(\frac{-3}{p})}{2},$$

代表曲线

$$y^2 = (x^2-1)(x^2-a^2)(x^2-b^2),$$

长二阶元只有 $\sigma : x \to -x$.

(3) $\mathrm{RA}(C) = S_3$, 超特殊曲线个数

$$n_2 = \frac{p-1}{6} - \frac{1-(\frac{-2}{p})}{2} - \frac{1-(\frac{-3}{p})}{3},$$

代表曲线

$$y^2 = (x^3-1)(x^3-a^3),$$

长二阶元有三个 $\sigma : x \to \frac{a}{x}, \frac{\omega a}{x}, \frac{\omega^2 a}{x}$. (其中 ω 为三次单位根.)

(4) $\mathrm{RA}(C) = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, 超特殊曲线个数

$$n_3 = \frac{p-1}{8} - \frac{1-(\frac{-1}{p})}{8} - \frac{1-(\frac{-2}{p})}{4} - \frac{1-(\frac{-3}{p})}{2},$$

代表曲线

$$y^2 = x(x^2-1)(x^2-a^2),$$

长二阶元有两个 $\sigma : x \to \frac{a}{x}, \frac{-a}{x}$.

(5) $\mathrm{RA}(C) = D_{12}$, 超特殊曲线个数

$$n_4 = \frac{1-(\frac{-3}{p})}{2},$$

代表曲线

$$y^2 = x^6 - 1,$$

长二阶元有四个 $\sigma : x \to -x, \frac{\zeta}{x}, \frac{\zeta^3}{x}, \frac{\zeta^5}{x}$. (其中 ζ 为六次单位根.)

(6) $\mathrm{RA}(C) = S_4$, 超特殊曲线个数

$$n_5 = \frac{1-(\frac{-2}{p})}{2},$$

代表曲线

$$y^2 = x(x^4 - 1),$$

长二阶元有六个 $\sigma : x \to \frac{x+1}{x-1}, -\frac{x-1}{x+1}, \frac{i(x+i)}{x-i}, \frac{i}{x}, -\frac{i}{x}, -\frac{i(x-i)}{x+i}$. (其中 i 为四次单位根.)

(7) $\mathrm{RA}(C) = \mathbb{Z}/5\mathbb{Z}$, 超特殊曲线个数

$$n_6 = \begin{cases} 0, & p \equiv 1,2,3 \bmod 5, \\ 1, & p \equiv 4 \bmod 5, \end{cases}$$

代表曲线

$$y^2 = x^5 - 1,$$

没有长二阶元.

3. 从雅可比簇出发的 Richelot 同源

定义 4.12　从 $\mathrm{Jac}(C)$ 出发到两条超奇异椭圆曲线乘积的 Richelot 同源称为分解同源.

定理 4.15　设 C 是亏格 2 的超椭圆曲线. 由 $\mathrm{Jac}(C)$ 出发的 15 条 Richelot 同源中分解同源的个数等于 $\mathrm{RA}(C)$ 中长二阶元的个数.

证明　证明参考 [33]. □

由于分解同源个数取决于长二阶元的个数, 可以通过计算长二阶元以及其在核中元素上的作用 (长二阶元作用在核上是否像), 来得到同源图的分类.

定理 4.16　设 C 是亏格 2 的超椭圆曲线. 由 Jac(C) 出发的 15 条 Richelot 同源如下分类：

(1) RA(C) = 0 时, 有 15 条不同的同源连接到雅可比簇.

(2) RA(C) = $\mathbb{Z}/2\mathbb{Z}$ 时, 有 6 条不同的同源连接到雅可比簇, 有 8 条同源以两重边的形式连接到雅可比簇, 还有 1 条同源连接到两个超奇异椭圆曲线的乘积.

(3) RA(C) = S_3 时, 有 3 条不同的同源连接到雅可比簇, 有 9 条同源以三重边的形式连接到雅可比簇, 还有 3 条同源以三重边连接到超奇异椭圆曲线的乘积.

(4) RA(C) = $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ 时, 有 1 条同源连接到雅可比簇, 有 8 条同源以两重边的形式连接到雅可比簇, 有 4 条同源以四重边的形式连接到雅可比簇, 还有 2 条同源连接到超奇异椭圆曲线的乘积.

(5) RA(C) = D_{12} 时, 有 2 条同源以两重边的形式连接到雅可比簇, 有 3 条同源以三重边的形式连接到雅可比簇, 有 6 条同源以六重边的形式连接到雅可比簇, 还有 1 条同源连接到超奇异椭圆曲线的乘积, 3 条同源以三重边的形式连接到超奇异椭圆曲线的乘积.

(6) RA(C) = S_4 时, 有 1 条同源连接到雅可比簇, 有 8 条同源以四重边的形式连接到雅可比簇, 有 6 条同源以六重边的形式连接到超奇异椭圆曲线的乘积.

(7) RA(C) = $\mathbb{Z}/5\mathbb{Z}$ 时, 有 15 条同源以五重边的形式连接到雅可比簇.

证明　证明参考 [33]. □

4. 从超奇异椭圆曲线乘积出发的 Richelot 同源

与椭圆曲线一样, 我们需要区分超奇异椭圆曲线的 j-不变量是否是 0 和 1728.

记 E, E' 为 j-不变量不等于 0 和 1728 的超奇异椭圆曲线, 由定理 2.4, $\mathrm{Aut}(E) = \mathrm{Aut}(E') = \{\pm 1\}$. 设 $E_2 : y^2 = x^3 - x$ 是 j-不变量等于 1728 的超奇异椭圆曲线, $E_3 : y^2 = x^3 - 1$ 是 j-不变量等于 0 的超奇异椭圆曲线. 则有其约化自同构群阶数为：

(1) $|\,\mathrm{RA}(E \times E')\,| = 1$;

(2) $|\,\mathrm{RA}(E \times E)\,| = 2$;

(3) $|\,\mathrm{RA}(E \times E_2)\,| = 2$;

(4) $|\,\mathrm{RA}(E \times E_3)\,| = 3$;

(5) $|\,\mathrm{RA}(E_2 \times E_2)\,| = 8$;

(6) $|\,\mathrm{RA}(E_3 \times E_3)\,| = 18$;

(7) $|\,\mathrm{RA}(E_2 \times E_3)\,| = 6$.

定理 4.17　从两条超奇异椭圆曲线乘积出发的 15 条 Richelot 同源如下分类：

(1) 当 $E \times E'$ 时, 6 条同源连接到雅可比簇, 9 条同源连接到两个超奇异椭圆曲线的乘积.

(2) 当 $E \times E$ 时, 3 条同源连接到雅可比簇, 2 条同源以两重边的形式连接到雅可比簇, 4 条同源连接到两个超奇异椭圆曲线的乘积, 6 条同源以两重边的形式连接到超奇异椭圆曲线的乘积.

(3) 当 $E \times E_2$ 时, 6 同源以两重边的形式连接到的雅可比簇, 3 条同源连接到超奇异椭圆曲线的乘积, 6 条同源以两重边的形式连接到超奇异椭圆曲线的乘积.

(4) 当 $E \times E_3$ 时, 6 条同源以三重边的形式连接到两个雅可比簇, 9 条同源以三重边的形式连接到超奇异椭圆曲线的乘积.

(5) 当 $E_2 \times E_2$ 时, 4 条同源以四重边的形式连接到雅可比簇, 1 条同源连接到超奇异椭圆曲线的乘积, 2 条同源以两重边重边的形式连接到超奇异椭圆曲线的乘积, 8 条同源以四重边的形式连接到超奇异椭圆曲线的乘积.

(6) 当 $E_3 \times E_3$ 时, 3 条同源以三重边的形式连接到雅可比簇, 3 条同源以三重边的形式连接到超奇异椭圆曲线的乘积, 9 条同源以九重边的形式连接到超奇异椭圆曲线的乘积.

(7) 当 $E_2 \times E_3$ 时, 6 条同源以六重边的形式连接到雅可比簇, 3 条同源以三重边的形式连接到超奇异椭圆曲线的乘积, 6 条同源以六重边的形式连接到超奇异椭圆曲线的乘积.

证明　证明参考 [33]. □

4.3.4　超特殊主极化阿贝尔簇 (ℓ,ℓ) 同源图

1. (ℓ,ℓ)-同源图的定义

定义 4.13　设 A_1, A_2 为定义在 $\overline{\mathbb{F}}_p$ 上的二维超特殊主极化阿贝尔簇. 若同源 $\phi : A_1 \to A_2$ 满足 $\ker(\phi) = \mathbb{Z}/\ell\mathbb{Z} \times \mathbb{Z}/\ell\mathbb{Z}$, 则称其为 (ℓ,ℓ)-同源. 此时存在 $\hat{\phi} \circ \phi = [\ell]$.

定义 4.14　超特殊 (ℓ,ℓ)-同源图 $\mathcal{G}_{p,\ell}$ 的顶点集由所有的 2 维超特殊主极化阿贝尔簇 $\overline{\mathbb{F}}_p$ 同构类组成, 对于图中的两点 $[A_1], [A_2]$, 连接 $[A_1]$ 到 $[A_2]$ 之间的一条边是指一个 (ℓ,ℓ)-同源的等价类, 两个 (ℓ,ℓ)-同源等价是指它们有相同的核.

超特殊 (ℓ,ℓ)-同源图和超特殊 Richelot 同源图的顶点集相同. 对于边则有如下结果:

命题 4.18　图 $\mathcal{G}_{p,\ell}$ 中每个顶点的极大 ℓ-韦伊迷向子群的个数是 $(\ell+1)(\ell^2+1)$, 从而输出边的个数是 $(\ell+1)(\ell^2+1)$.

证明　可以参考 [34] 命题 8. □

2. (ℓ,ℓ) 同源图的记号

在这里 s 首先考虑一般的 g 维的阿贝尔簇. 设 A 为一个阿贝尔簇, P 为其上的主极化除子, $\mathcal{A}=(A,P)$ 为主极化阿贝尔簇.

由于 g 维超特殊阿贝尔簇 A 同构于超奇异椭圆曲线的乘积, 那么超特殊阿贝尔簇的自同态环同构于 $M_g(\mathcal{O})$, 其中 $\mathcal{O}$ 为任一超奇异椭圆曲线的自同态环即为四元数代数 $B_{p,\infty}$ 的极大阶.

记

(1) $\mathrm{Iso}_n(\mathcal{A})=$ {极大 n-韦伊迷向子群 $C\subseteq\mathcal{A}[n]$}, $\mathrm{N}(\mathcal{A},n)=\#\mathrm{Iso}_n(\mathcal{A})$.

(2) $\mathrm{SS}(g,p)$ 为 g 维超特殊阿贝尔簇同构类集合, $h(g,p)=\#\mathrm{SS}(g,p)$.

(3) $\mathscr{M}=M_g(\mathcal{O})\cong\mathrm{End}_{\overline{\mathbb{F}}_p}(A)$.

(4) $\mathscr{M}^\times=SL_g(\mathcal{O})$.

(5) $\mathcal{H}=\{H\in\mathscr{M}\mid H$ 正定且有约化范数 1$\}$.

3. $\mathrm{SS}(g,p)$ 的对应关系

固定一个主极化除子 X, 考虑 (3.5)

$$j:\mathrm{NS}(A)=\mathrm{Pic}(A)/\mathrm{Pic}^0(A)\to\mathrm{End}(A)\cong M_g(\mathcal{O});\qquad \overline{L}\to\phi_X^{-1}\circ\phi_L,$$

其中 $\mathcal{O}$ 为四元数代数 $B_{p,\infty}$ 的极大序.

将阿贝尔簇的自同态 α 对应到矩阵环 M, 则有 Rosati 对合后 $\alpha^\dagger$ 对应矩阵的共轭转置 M^+.

由命题 3.19可知,

$$j(\bar{L})=j(\bar{L})^+,$$

其中 $j(\bar{L})^+$ 为 $j(\bar{L})$ 的共轭转置.

命题 4.19

$$\frac{L^g}{g!}=\chi(L)=\mathrm{HNm}(j(\bar{L})),\qquad \chi(L)^2=\deg(\phi_L).$$

且

(1) L 为强的 (L 对应极化除子) 当且仅当 $j(\bar{L})$ 正定的.

(2) L 为主极化除子当且仅当 $j(\bar{L})$ 正定的且 $\deg(\phi_L)=1$ 当且仅当 $j(\bar{L})$ 正定的且 $j(\bar{L})$ 的约化范数是 1.

其中 HNm 为约化范数, 特别的, 当 $g=2$ 时, $\mathrm{HNm}(j(\bar{L}))=\det(j(\bar{L}))$.

证明　参考 [60] 命题 2.8. □

命题 4.20　当 $g=2$ 时, 对任意正整数 d, 有

$$\{\bar{L}\in\mathrm{NS}(A)\mid L>0,L^2=2d\}\to\{\begin{pmatrix}a & b\\ \bar{b} & c\end{pmatrix}\in M_2(\mathcal{O})\mid a,c\in\mathbb{Z},a>0,c>0,ac-b\bar{b}=d\}$$

$$\bar{L} \qquad \to \qquad \phi_X^{-1} \circ \phi_L$$

是一一对应.

证明　参考 [60] 推论 2.9. □

定理 4.21　对于 $\mathscr{M}$ 作用在 $\mathcal{H}$ 上有：$\mathscr{M} \times \mathcal{H} \to \mathcal{H}; (M, H) \to M^+ H M$.
H 与 $M^+ H M$ 对应同一主极化除子, 从而有 $\mathcal{H}/\mathscr{M}^\times$ 与 $\mathrm{SS}(g, p)$ 一一对应.

证明　参考 [34] 命题 4. □

定理 4.22　超特殊主极化阿贝尔簇的 (ℓ, ℓ) 同源 $\alpha : \mathcal{A}_1 = (A, H_1) \to \mathcal{A}_2 = (A, H_2)$ 对应矩阵 $M \in M_2(\mathcal{O})$, 使得 $M^+ H_2 M = \ell H_1$.

证明　设 H_1 对应的主极化除子是 P_1, H_2 对应的主极化除子是 P_2. 先来证明

$$\lambda_{\alpha^*(P_2)} = \hat{\alpha} \circ \lambda_{P_2} \circ \alpha.$$

对于任意的 $a \in A$, 我们有：

$$\hat{\alpha} \circ \lambda_{P_2} \circ \alpha(a) = \hat{\alpha}(t^*_{\alpha(a)} P_2 - P_2) = \alpha^* t^*_{\alpha(a)} P_2 - \alpha^* P_2 = (t_{\alpha(a)} \circ \alpha)^* P_2 - \alpha^* P_2.$$

另一方面, 由于 $t_{\alpha(a)} \circ \alpha = \alpha \circ t_a$, 则：

$$\hat{\alpha} \circ \lambda_{P_2} \circ \alpha(a) = (\alpha \circ t_a)^* P_2 - \alpha^* P_2 = t_a^* \alpha^* P_2 - \alpha^* P_2 = \lambda_{\alpha^*(P_2)}(a).$$

从而

$$\lambda_{\alpha^*(P_2)} = \hat{\alpha} \circ \lambda_{P_2} \circ \alpha.$$

由定理 3.18, $\alpha^*(P_2) \sim \ell P_1$, 则

$$\lambda_{\ell P_1} = \hat{\alpha} \circ \lambda_{P_2} \circ \alpha.$$

进一步,

$$\lambda_{\ell P_1} = \lambda_X \circ \ell H_1, \qquad \lambda_{P_2} = \lambda_X \circ H_2.$$

综上有：

$$\lambda_X \circ \ell H_1 = \hat{\alpha} \circ \lambda_X \circ H_2 \circ \alpha.$$

将 λ_X 取逆, 有:

$$\ell H_1 = \lambda_X^{-1} \circ \hat{\alpha} \circ \lambda_X \circ H_2 \circ \alpha = \alpha^\dagger \circ H_2 \circ \alpha = M^+ H_2 M.$$

□

定理 4.23　设 $\mathcal{A} = (A, P)$ 为 g 维的主极化超特殊阿贝尔簇, 则：

(1) ℓ 为一个素数且 $\ell \neq p$, 则有 $\mathrm{N}(\mathcal{A}, \ell) = \prod_{k=1}^{g} (\ell^k + 1)$.

(2) 对于 m, n 为整数且 $(m, n) = 1$, 则 $\mathrm{N}(\mathcal{A}, mn) = \mathrm{N}(\mathcal{A}, m)\,\mathrm{N}(\mathcal{A}, n)$.

证明　证明参考 [34] 命题 8. □

第 5 章　同源图在密码学中的应用

5.1　椭圆曲线同源图在密码学中的应用

超奇异椭圆曲线同源计算在后量子密码中主要有如下三个方面的应用：

(1) CGL-哈希函数

(2) SIDH 密钥交换协议

(3) CSIDH 密钥交换协议

5.1.1　CGL-哈希函数

CGL-哈希函数是由 Charles-Lauter-Goren[5] 根据超奇异椭圆曲线同源图的路径寻找问题设计的哈希函数. 这里的哈希函数是从有限长的比特串到 $\overline{\mathbb{F}}_p$ 上的超奇异椭圆曲线的 j-不变量的函数.

考虑 $\overline{\mathbb{F}}_p$ 上的超奇异 2-同源图 $\mathcal{G}_2(\overline{\mathbb{F}}_p)$, 由于每个顶点输出边个数是 3, 则对于每个顶点 $[E_{-1}]$, 取一个同源

$$\phi : E_{-1} \to E_0,$$

此时除了 $\hat{\phi}$ 之外还有两条从 E_0 出发的 2-同源, 记为

$$\phi_1^0 : E_0 \to E_1^{(0)}, \qquad \phi_1^1 : E_0 \to E_1^{(1)}.$$

如果我们给定的比特串是 $m = m_1 \cdots m_n$, 其中 $m_i \in \{0, 1\}$, 则取

$$\phi_1^{m_1} : E_0 \to E_1^{(m_1)},$$

记 $E_1 = E_1^{(m_1)}$, 继续取除了 $\hat{\phi}_1^{m_1}$ 之外的两条 2-同源, 记为

$$\phi_2^0 : E_1 \to E_2^{(0)}, \qquad \phi_2^1 : E_1 \to E_2^{(1)}.$$

此时取

$$\phi_2^{m_2} : E_1 \to E_2^{(m_2)},$$

并记 $E_2 = E_2^{(m_2)}$. 如此一直进行下去, 最终我们由 m_n 得到 E_n, 输出 E_n 的 j-不变量即比特串的哈希值. 这样就定义哈希函数

$$H : m_1 \cdots m_n \to j(E_n).$$

熟知哈希函数的安全性依赖于以下问题的困难性：对于给定的哈希函数 $H : A \to B$,

(1) 第一原像寻找：给定 $b \in B$, 是否可以找到 $a \in A$ 使得 $H(a) = b$?

(2) 第二原像寻找：给定 $a_1 \in A$, 是否可以找到 $a_2 \in A$ 使得 $H(a_1) = H(a_2)$?

(3) 碰撞性：给定 $b \in B$, 是否可以找到 $a_1, a_2 \in A$ 使得 $H(a_1) = H(a_2)$?

(4) 不可区分性：能否区分 $\{H(a) \mid$ 随机的 $a \in A\}$ 和 $\{H(b) \mid$ 随机的 $b \in B\}$?

攻击 CGL-哈希函数的方法主要有生日攻击, Frobenius 攻击, 找回路攻击和找圈和环路的攻击. 攻击的关键在于如何在超奇异椭圆曲线同源图中寻找同源, 即寻找随机游走, 而它依赖于对同源图的研究, 比如找环路和邻域等.

超奇异椭圆曲线同源图是连通的 $\ell + 1$ 正则图, 从而有拉马努金性质, 即很好的随机性质, 可以在其中寻找路径. 关于拉马努金图在密码学中的应用用可以参考 [61].

2018 年, Eisentrager-Hallgren-Lauter-Morrison-Petit[25] 指出计算超奇异椭圆曲线之间的同源问题和计算超奇异椭圆曲线的自同态环问题是等价的, 这些问题也和 CGL 哈希函数中的第一原像寻找和碰撞问题是等价的.

2020 年, Eisenträger-Hallgren-Leonardi-Morrison-Park[20] 通过找到超奇异椭圆曲线中的两个自同态来生成自同态环, 其计算复杂度是 $O(p^{\frac{1}{2}} log^2 p) = \tilde{O}(p^{\frac{1}{2}})$. 这一结果也攻击了哈希函数中的第二原像寻找问题.

5.1.2　SIDH 密钥交换协议

SIDH 是由 Jao-De Feo[7] 设计的基于超奇异同源的 Diffie-Hellman 密钥交换协议.

(1) 参数选取：取定素数

$$p = \ell_A^{e_A} \ell_B^{e_B} f - 1,$$

其中 ℓ_A, ℓ_B 为两个小的素数, f 为与其互素的数 (一般取 $\ell_A = 2, \ell_B = 3$, 且 $\ell_A^{e_A} \approx \ell_B^{e_B}$).

E 为 $\mathbb{F}_{p^2}$ 上的超奇异椭圆曲线, 且

$$E[\ell_A^{e_A}] = \langle P_A, Q_A \rangle, E[\ell_B^{e_B}] = \langle P_B, Q_B \rangle.$$

(2) 私钥选择: Alice 选择私钥

$$a \in \{0, \cdots, \ell_A^{e_A} - 1\},$$

此时选择循环子群

$$G_A = \langle P_A + [a] Q_A \rangle.$$

计算同源

$$\phi_A : E \to E_A = E/G_A.$$

同样的, Bob 做相同的事情, 选择私钥

$$b \in \{0, \cdots, \ell_B^{e_B} - 1\},$$

此时选择循环子群

$$G_B = \langle P_B + [b]Q_B \rangle.$$

计算同源

$$\phi_B : E \to E_B = E/G_B.$$

(3) 进行交换: Alice 和 Bob 都公开

$$\{E_A, \phi_A(P_B), \phi_A(Q_B)\}$$

和

$$\{E_B, \phi_B(P_A), \phi_B(Q_A)\}.$$

从而 Alice 根据 Bob 公开的计算子群

$$G'_A = \langle \phi_B(P_A) + [a]\phi_B(Q_A) \rangle,$$

用这个子群计算同源

$$\phi_{BA} : E_B \to E_{BA} = E_B/G'_A \cong E/\langle G_A, G_B \rangle.$$

同样的, Bob 做相同的事情, 根据 Alice 公开的计算子群

$$G'_B = \langle \phi_A(P_B) + [b]\phi_A(Q_B) \rangle,$$

用这个子群计算同源

$$\phi_{AB} : E_A \to E_{AB} = E_A/G'_B \cong E/\langle G_A, G_B \rangle.$$

这时, Alice 和 Bob 输出其对应的椭圆曲线 E_{BA} 和 E_{AB} 的 j-不变量. 这两者是一致的, 即完成了交换.

SIDH 的安全性依赖于计算两个超奇异椭圆曲线间的同源是困难的, Biasse-Jao-Sankar[10] 在 2014 年提出了一个算法, 先将在 $\mathbb{F}_{p^2}$ 上的超奇异椭圆曲线通过量子的 Grover 算法找到到定义在 $\mathbb{F}_p$ 上的超奇异椭圆曲线的同源, 其时间复杂度是 $O(p^{\frac{1}{4}})$. 而计算定义在 $\mathbb{F}_p$ 上的超奇异椭圆曲线的同源的时间复杂度是亚指数的. 所以在量子算法下改进从 $\mathbb{F}_{p^2}$ 上的超奇异椭圆曲线到定义在 $\mathbb{F}_p$ 上的超奇异椭圆曲线的同源的寻找是其中的关键. 总之, 计算超奇异椭圆曲线同源在量子计算机下时间复杂度是指数时间.

5.1.3　CSIDH 密钥交换

CSIDH 是由 Castryck-Lange-Martindale-Panny-Renes[8] 设计的基于超奇异同源的可交换的 Diffie-Hellman 密钥交换协议. 这个协议的数学基础是定理 4.7, 即 $\mathrm{Cl}(\mathcal{O})$ 在 $\mathrm{Ell}_{\mathcal{O}}(\mathbb{F}_p)$ 上的作用是自由可迁的, 而且是交换的.

(1) 参数选取：取定素数

$$p = 4\ell_1 \cdots \ell_n - 1,$$

其中 ℓ_i 为小的奇素数.

E 为定义在 $\mathbb{F}_p$ 上的超奇异椭圆曲线, $\mathrm{End}_{\mathbb{F}_p}(E) = \mathbb{Z}[\pi]$. 并取 m 为一个正整数满足

$$(2m+1)^n \leqslant \#\mathrm{Cl}(\mathbb{Z}[\pi]).$$

(2) 私钥选择：Alice 选择

$$(e_1, \cdots, e_n) \in \{-m, \cdots m\}^n,$$

对应理想

$$[I_A] = [\mathfrak{l}_1^{e_1} \cdots \mathfrak{l}_n^{e_n}],$$

其中 $\mathfrak{l}_i = \langle \ell_i, \pi - 1 \rangle$. 计算

$$\phi_A : E \to E_A = E/E[I_A].$$

同样的, Bob 做相同的事情, 选择私钥

$$(e'_1, \cdots, e'_n) \in \{-m, \cdots m\}^n,$$

对应理想

$$[I_B] = [\mathfrak{l}_1^{e'_1} \cdots \mathfrak{l}_n^{e'_n}],$$

其中 $\mathfrak{l}_i = \langle \ell_i, \pi - 1 \rangle$. 计算

$$\phi_B : E \to E_B = E/E[I_B].$$

(3) 进行交换：Alice 和 Bob 都公开

$$E_A = [I_A]E$$

和

$$E_B = [I_B]E.$$

从而 Alice 根据 Bob 公开的 E_B 计算

$$[I_A]E_B = [I_A][I_B]E.$$

同样的, Bob 做相同的事情, 根据 Alice 公开的 E_A 计算

$$[I_B]E_A = [I_B][I_A]E.$$

这时, Alice 和 Bob 输出其对应的椭圆曲线的 j-不变量, 由交换性, 如果得到的一致即完成了交换.

CSIDH 的安全性也依赖于椭圆曲线同源的计算, 当然和理想的作用也有很大的关系, 类似于理想类群的离散对数问题.

5.1.4　与密码学问题有关的数学问题

(1) 计算给定椭圆曲线的自同态环：给定素数 p 和其上的超奇异椭圆曲线 E 的 j-不变量, 能否找到 $\alpha_1, \alpha_2, \alpha_3, \alpha_4 \in B_{p,\infty}$ 使得 $\mathrm{End}(E) = \mathbb{Z}\alpha_1+\mathbb{Z}\alpha_2+\mathbb{Z}\alpha_3+\mathbb{Z}\alpha_4$?

(2) 计算给定两条超奇异椭圆曲线的同源: 给定两条超奇异椭圆曲线 E_1, E_2, 如何计算一条同源 $\phi : E_1 \to E_2$ 次数是 ℓ^n? 即为路径寻找的问题.

(3) 计算超奇异椭圆曲线的同源图: 对于超奇异椭圆曲线同源图中的点, 如何计算其对应的环路和邻域?

这些问题是等价的[25], 也是对上面三个密码学应用做密码分析的关键.

5.2　阿贝尔簇同源图在密码学中的应用

随着超奇异椭圆曲线在密码学中的应用的深入, 密码学家提出了基于二维的阿贝尔簇的同源密码体制, 当前有两个主要算法应用：

(1) 哈希函数

(2) 亏格 2 的 SIDH 密钥交换协议

5.2.1　基于阿贝尔簇的哈希函数

基于阿贝尔簇的哈希函数是由 Castryck-Decru-Smith[32] 根据超特殊阿贝尔簇的 Richelot 同源图的路径的寻找问题而设计的哈希函数.

由于两条椭圆曲线的乘积不容易计算不变量, 所以希望同源像是超椭圆曲线的雅可比簇. 从而考虑 $(2,2)$-同源 $\phi_1 : A_0 \to A_1$, 对于 $\phi_2 : A_1 \to A_2$ 有以下情况：

(1) 当 $\phi_2 = \hat{\phi_1}$ 时, $\ker(\phi_2 \circ \phi_1) \cong (\mathbb{Z}/2\mathbb{Z})^4$, 即 $\phi_2 \circ \phi_1$ 为 $(2,2,2,2)$-同源. 则称 ϕ_2 为 ϕ_1 的对偶扩张.

(2) 当 $\ker(\phi_2 \circ \phi_1) \cong \mathbb{Z}/4\mathbb{Z} \times (\mathbb{Z}/2\mathbb{Z})^2$ 时, 即 $\phi_2 \circ \phi_1$ 为 $(4,2,2)$-同源. 则称 ϕ_2 为 ϕ_1 的坏扩张. 坏扩张有 6 条.

(3) 当 $\ker(\phi_2 \circ \phi_1) \cong (\mathbb{Z}/4\mathbb{Z})^2$ 时, 即 $\phi_2 \circ \phi_1$ 为 $(4,4)$-同源. 则称 ϕ_2 为 ϕ_1 的好扩张. 好扩张有 8 条.

通过计算可以得到, 无论是两条椭圆曲线的乘积还是超椭圆曲线的雅可比簇, 由其出发的 $(2,2)$-同源只有当是好同源时才会到达超椭圆曲线的雅可比簇, 所以选择同源时有 8 条选择, 故选择 3 比特对应一条边. 此时哈希函数是

$$H:\{\text{有限长的比特串}\}\to\{\text{超椭圆曲线的 Igusa-Clebsch 不变量}[I_2,I_4,I_6,I_{10}]\}.$$

这里具体的过程和椭圆曲线类似, 但是每条边 (路径) 对应 3 比特.

同样的, 攻击的关键是确定二维超特殊阿贝尔簇的 Richelot 同源图, 即找环路和邻域等.

5.2.2　亏格 2 的 SIDH

亏格 2 的 SIDH 是由 Flyyn-Ti[31] 设计的基于亏格 2 的超椭圆曲线的 Diffie-Hellman 密钥交换协议.

首先对于超椭圆曲线 C 的雅可比簇 $\mathrm{Jac}(C)$,

$$\mathrm{Jac}(C)[\ell^n]=\langle P_1,P_2,P_3,P_4\rangle.$$

如何找到极大 ℓ^n-韦伊迷向子群是同构于 $\mathbb{Z}/\ell^n\mathbb{Z}\times\mathbb{Z}/\ell^{n-k}\mathbb{Z}\times\mathbb{Z}/\ell^k\mathbb{Z}$. 方式如下：

(1) 先找到 $a_{i,j}$ 使得

$$e_{\ell^n}(P_i,P_j)=e_{\ell^n}(P_1,P_2)^{a_{i,j}}.$$

并选择

$$r_1,r_2,r_3,r_4\in\{0,\cdots\ell^n-1\}$$

且与 ℓ 互素.

(2) 进一步, 计算

$$t_1,t_2,t_3,t_4,s_1,s_2,s_3,s_4$$

使得:

$$\begin{aligned}r_1s_2-r_2s_1+a_{1,3}(r_1s_3-r_3s_1)+a_{1,4}(r_1s_4-r_4s_1)+a_{2,3}(r_2s_3-r_3s_2)\\+a_{2,4}(r_2s_4-r_4s_2)+a_{3,4}(r_3s_4-r_4s_3)\equiv 0 \bmod \ell^k;\end{aligned}\tag{5.1}$$

$$\begin{aligned}r_1t_2-r_2t_1+a_{1,3}(r_1t_3-r_3t_1)+a_{1,4}(r_1t_4-r_4t_1)+a_{2,3}(r_2t_3-r_3t_2)\\+a_{2,4}(r_2t_4-r_4t_2)+a_{3,4}(r_3t_4-r_4t_3)\equiv 0 \bmod \ell^{n-k}.\end{aligned}\tag{5.2}$$

(3) 取

$$Q_1=\sum_{i=1}^{4}[s_i]P_i,\qquad Q_2=\sum_{i=1}^{4}[r_i]P_i,\qquad Q_3=\sum_{i=1}^{4}[t_i]P_i.$$

则有

$$\langle Q_1,Q_2,Q_3\rangle\cong\mathbb{Z}/\ell^n\mathbb{Z}\times\mathbb{Z}/\ell^{n-k}\mathbb{Z}\times\mathbb{Z}/\ell^k\mathbb{Z}.$$

亏格 2 的 SIDH 密钥交换如下：

(1) 参数选取：取定素数

$$p = \ell_A^{e_A}\ell_B^{e_B} f - 1,$$

其中 ℓ_A, ℓ_B 为两个小的素数, f 为与其互素的数. (一般取 $\ell_A = 2, \ell_B = 3$, 且 $\ell_A^{e_A} \approx \ell_B^{e_B}$)

超椭圆曲线 C 的雅可比簇 Jac(C),

$$\mathrm{Jac}(C)[2^{e_A}] = \langle P_1, P_2, P_3, P_4\rangle, \qquad \mathrm{Jac}(C)[3^{e_B}] = \langle Q_1, Q_2, Q_3, Q_4\rangle$$

(2) 私钥选择：Alice 选择私钥 $(a_i)_{i=1}^{12}$, 对应子群

$$G_A = \langle \sum_{i=1}^{4}[a_i]P_i, \sum_{i=5}^{8}[a_i]P_{i-4}, \sum_{i=9}^{12}[a_i]P_{i-8}\rangle$$

(由上面的步骤可以保证这个子群是极大 2^n-韦伊迷向子群), 然后计算同源

$$\phi_A : \mathrm{Jac}(C) \to \mathrm{Jac}(C_A).$$

同样的, Bob 做相同的事情, 选择私钥 $(b_i)_{i=1}^{12}$, 对应子群

$$G_B = \langle \sum_{i=1}^{4}[b_i]Q_i, \sum_{i=5}^{8}[b_i]Q_{i-4}, \sum_{i=9}^{12}[b_i]Q_{i-8}\rangle$$

(由上面的步骤可以保证这个子群是极大 3^n-韦伊迷向子群), 然后计算同源

$$\phi_B : \mathrm{Jac}(C) \to \mathrm{Jac}(C_B).$$

(3) 进行交换: Alice 和 Bob 都公开

$$\{\mathrm{Jac}(C_A), \phi_A(Q_1), \phi_A(Q_2), \phi_A(Q_3), \phi_A(Q_4)\}$$

和

$$\{\mathrm{Jac}(C_B), \phi_B(P_1), \phi_B(P_2), \phi_B(P_3), \phi_B(P_4)\}.$$

从而 Alice 根据 Bob 公开的子群计算

$$G'_A = \langle \sum_{i=1}^{4}[a_i]\phi_B(P_i), \sum_{i=5}^{8}[a_i]\phi_B(P_{i-4}), \sum_{i=9}^{12}[a_i]\phi_B(P_{i-8})\rangle$$

用这个子群计算同源

$$\phi_{BA} : \mathrm{Jac}(C_B) \to \mathrm{Jac}(C_{BA}) = \mathrm{Jac}(C_B)/G'_A \cong \mathrm{Jac}(C)/\langle G_A, G_B\rangle.$$

同样的, Bob 做相同的事情, 根据 Alice 公开的计算子群

$$G'_B = \langle \sum_{i=1}^{4} [b_i]\phi_A(Q_i), \sum_{i=5}^{8} [b_i]\phi_A(Q_{i-4}), \sum_{i=9}^{12} [b_i]\phi_A(Q_{i-8}) \rangle$$

用这个子群计算同源

$$\phi_{AB} : \mathrm{Jac}(C_A) \to \mathrm{Jac}(C_{AB}) = \mathrm{Jac}(C_A)/G'_B \cong \mathrm{Jac}(C)/\langle G_A, G_B \rangle.$$

这时, Alice 和 Bob 输出其对应的超椭圆曲线的雅可比簇 $\mathrm{Jac}(C_{BA})$ 和 $\mathrm{Jac}(C_{AB})$ 的 Igusa-Clebsch 不变量. 如果得到的一致即完成了交换.

当然这里亏格 2 的 SIDH 安全性基于二维超奇异主极化阿贝尔簇的同源计算问题, 尤其是两条超椭圆曲线的雅可比簇之间的同源计算问题, 这也是高维阿贝尔簇上的 SIDH 密码分析的关键.

第 6 章　椭圆曲线同源图的主要结果

回忆在第二章最后, $j = 1728$ 的超奇异椭圆曲线 E_{1728} (此时 $p \equiv 3 \bmod 4$) 的自同态环

$$\mathcal{O}_{1728} = \mathbb{Z} + \mathbb{Z}i + \mathbb{Z}\frac{1+j}{2} + \mathbb{Z}\frac{i+k}{2},$$

其中 $i^2 = -1, j^2 = -p$.

同 $j = 1728$ 的情形一样, $j = 0$ 的超奇异椭圆曲线 E_0 (此时 $p \equiv 2 \bmod 3$) 的自同态环

$$\mathcal{O}_0 = \mathbb{Z} + \mathbb{Z}\frac{1+i}{2} + \mathbb{Z}\frac{i+k}{3} + \mathbb{Z}\frac{j+k}{2},$$

其中 $i^2 = -3, j^2 = -p$.

在本章, 我们用 $\mathcal{O}_{1728}$ 代表 E_{1728} 的自同态环, 用 $\mathcal{O}_0$ 代表 E_0 的自同态环. 我们将证明论文的主要结果.

6.1　超奇异椭圆曲线同源图中 $j = 0, 1728$ 环路的个数

根据 Deuring 对应定理 2.27，环路对应的是是自同态环的左主理想，所以计算 ℓ 同源的环路的个数，就是计算自同态环约化范数是 ℓ 的等价元素的个数, 这转化为求解丢番图方程的问题，

定理 6.1　[21][22] 在超奇异椭圆曲线同源图 $G_\ell(\overline{\mathbb{F}}_p)$ 中,

(1) 对于 j-不变量是 1728 的超奇异椭圆曲线 E_{1728} ($p \equiv 3 \bmod 4$), 当 $p > 4\ell$ 时, 在顶点 $[E_{1728}]$ 处
   (i) 当 $\ell \equiv 1 \bmod 4$ 时, 有两条环路;
   (ii) 当 $\ell \equiv 3 \bmod 4$ 时, 没有环路;
   (iii) 当 $\ell = 2$ 时, 有一条环路.

(2) 对于 j-不变量是 0 的超奇异椭圆曲线 $E_0(p \equiv 2 \bmod 3)$, 当 $p > 3\ell$ 时, 在顶点 $[E_0]$ 处有
   (i) 当 $\ell \equiv 1 \bmod 3$ 时, 有两条环路;
   (ii) 当 $\ell \equiv 2 \bmod 3$ 时, 没有环路;
   (iii) 当 $\ell = 2$ 时, 没有环路;
   (iv) 当 $\ell = 3$ 时, 有一条环路.

证明　(1) 考虑 E_{1728}, 由 Deuring 对应定理 2.27, 从 E_{1728} 出发的定义在 $\overline{\mathbb{F}}_p$ 上的到自身的 ℓ 同源对应到 $\mathrm{End}(E_{1728})$ 的约化范数是 ℓ 的左主理想. 所以在 $G_\ell(\overline{\mathbb{F}}_p)$ 中寻找 E_{1728} 的环路就相当于寻找 $\mathcal{O}_{1728}$ 约化范数是 ℓ 的左主理想, 即约化范数是 ℓ 的元素.

对于 $\mathcal{O}_{1728}$ 的左主理想

$$\langle a+bi+c\frac{1+j}{2}+d\frac{i+k}{2}\rangle,$$

其约化范数为

$$\mathrm{Nrd}(I)=\left(a+\frac{c}{2}\right)^2+\left(b+\frac{d}{2}\right)^2+\frac{pc^2}{4}+\frac{pd^2}{4}=\ell. \tag{6.1}$$

当 $p>4\ell$ 时, $(c,d)=(0,0)$, 方程变为

$$a^2+b^2=\ell. \tag{6.2}$$

在 $\mathbb{Q}(\sqrt{-1})$ 中, 由于其类数为 1, 所以 $\mathbb{Z}[\sqrt{-1}]$ 为 PID, 从而有理想唯一分解.

对于 $\mathbb{Q}[\sqrt{-1}]$ 中的每个整理想有形式

$$\langle a+b\sqrt{-1}\rangle,$$

且

$$\mathrm{N}(a+b\sqrt{-1})=a^2+b^2.$$

在相差一个单位的情况下, 方程 (6.2) 是否有解取决于 ℓ 在 $\mathbb{Q}[\sqrt{-1}]$ 是分裂的还是惯性的.

当 $\ell\equiv 3 \bmod 4$ 时, $\left(\frac{-1}{\ell}\right)=-1$, 即 ℓ 在 $\mathbb{Q}[\sqrt{-1}]$ 中惯性. 此时方程无解, 所以没有环路.

当 $\ell\equiv 1 \bmod 4$, $\left(\frac{-1}{\ell}\right)=1$, 即 ℓ 在 $\mathbb{Q}[\sqrt{-1}]$ 中分裂. 差一个单位的情况下, 有两组解, 即对应两个主理想 $\langle a+b\sqrt{-1}\rangle$, $\langle a-b\sqrt{-1}\rangle$. 这说明有两个定义在 $\overline{\mathbb{F}}_p$ 上从 E_{1728} 到 E_{1728} 的 ℓ-同源.

当 $\ell=2$ 时, 解为 $(\pm1,\pm1)$. 在差一个单位情况下, 有一组解, 即对应主理想 $\langle 1+\sqrt{-1}\rangle$. 这说明有一个定义在 $\overline{\mathbb{F}_p}$ 上从 E_{1728} 到 E_{1728} 的 2-同源.

(2) 考虑 E_0, 由 Deuring 对应定理 2.27, 从 E_0 出发的定义在 $\overline{\mathbb{F}_p}$ 上的到自身的 ℓ 同源对应到 $\mathrm{End}(E_0)$ 的约化范数是 ℓ 的左主理想. 所以在 $G_\ell(\overline{\mathbb{F}_p})$ 中找 E_0 的环路就相当于找约化范数是 ℓ 的左主理想, 即约化范数是 ℓ 的元素.

对于左主理想

$$\langle a+b\frac{-1+i}{2}+cj+d\frac{3+i+3j+k}{6}\rangle,$$

其约化范数为

$$\mathrm{Nrd}(I)=(a-\frac{b}{2}+\frac{d}{2})^2+3(\frac{b}{2}+\frac{d}{6})^2+p(c+\frac{d}{2})^2+3p(\frac{d}{6})^2=\ell. \tag{6.3}$$

又由

$$p(c+\frac{d}{2})^2+3p(\frac{d}{6})^2=p(c^2+cd+\frac{d^2}{3})=p[(c+\frac{d}{2})^2+\frac{d^2}{12}].$$

由于 $c,d\in\mathbb{Z}$, 若 $(c,d)\neq(0,0)$, $(c+\frac{d}{2})^2+\frac{d^2}{12}\geqslant\frac{1}{3}$. 因此当 $p\geqslant 3\ell$ 时,

$$p(c+\frac{d}{2})^2+3p(\frac{d}{6})^2\geqslant\frac{p}{3}>\ell.$$

综上当 $p>3\ell$ 时, $(c,d)=(0,0)$, 方程变为

$$(a-\frac{b}{2})^2+3(\frac{b}{2})^2=\ell, \tag{6.4}$$

在 $\mathbb{Q}(\sqrt{-3})$ 中, 由于其类数为 1, 所以 $\mathbb{Z}[\frac{1+\sqrt{-3}}{2}]$ 为 PID, 从而有理想唯一分解.

对于 $\mathbb{Q}[\sqrt{-3}]$ 中的每个整理想有形式

$$\langle -a+b\frac{1+\sqrt{-3}}{2}\rangle,$$

且

$$\mathrm{N}(-a+b\frac{1+\sqrt{-3}}{2})=(a-\frac{b}{2})^2+3(\frac{b}{2})^2.$$

在相差一个单位的情况下, 方程 6.4是否有解取决于 ℓ 在 $\mathbb{Q}[\sqrt{-3}]$ 是分裂的还是惯性的.

当 $\ell\equiv 2 \bmod 3\equiv 5 \bmod 6$ 时, $\left(\frac{-3}{\ell}\right)=-1$, 即 ℓ 在 $\mathbb{Q}[\sqrt{-3}]$ 中惯性. 此时方程无解, 所以没有环路.

当 $\ell\equiv 1 \bmod 3\equiv 1 \bmod 6$, $\left(\frac{-3}{\ell}\right)=1$, 即 ℓ 在 $\mathbb{Q}[\sqrt{-3}]$ 中分裂. 差一个单位的情况下, 有两组解, 即对应两个主理想 $\langle -a+b\frac{1+\sqrt{-3}}{2}\rangle$, $\langle -a+b\frac{1-\sqrt{-3}}{2}\rangle$. 这说明有两个定义在 $\overline{\mathbb{F}_p}$ 上从 E_0 到 E_0 的 ℓ-同源.

当 $\ell=2$ 时, ℓ 在 $\mathbb{Q}[\sqrt{-3}]$ 中惯性. 此方程无解. 这说明 E_0 没有环路. 当 $\ell=3$ 时, ℓ 在 $\mathbb{Q}[\sqrt{-3}]$ 中分歧. 在差一个单位的情况下, 有一组解, 对应理想 $\langle\sqrt{-3}\rangle$. 这说明有一个定义在 $\overline{\mathbb{F}_p}$ 上从 E_0 到 E_0 的 3-同源. □

定义 6.1

(1) 对于 $\ell\equiv 1 \bmod 4$, 定义 $p^1_{1728}(\ell)$ 为最大的满足 $p\equiv 3 \bmod 4$, $p\neq\ell$ 的素数使得 E_{1728} 至少有三条环路.

(2) 对于 $\ell\equiv 3 \bmod 4$, 定义 $p^3_{1728}(\ell)$ 为最大的满足 $p\equiv 3 \bmod 4$, $p\neq\ell$ 的素数使得 E_{1728} 至少有一条环路.

(3) 对于 $\ell\equiv 1 \bmod 3$, 定义 $p^1_0(\ell)$ 为最大的满足 $p\equiv 2 \bmod 3$, $p\neq\ell$ 的素数使得 E_0 至少有三条环路.

(4) 对于 $\ell\equiv 2 \bmod 3$, 定义 $p^2_0(\ell)$ 为最大的满足 $p\equiv 2 \bmod 3$, $p\neq\ell$ 的素数使得 E_0 至少有一条环路.

由表中数据我们可以看出:

(1) 比我们给出的界小时, 有：

表 6.1　$p^1_{1728}(\ell)$, $p^3_{1728}(\ell)$, $p^1_0(\ell)$, $p^2_0(\ell)$ **的值, 对于奇素数** $\ell \leqslant 283$

ℓ	3	5	7	11	13	17	19	23	29	31	37	41	43	47	53
$p^1_{1728}(\ell)$	-	19	-	-	47	67	-	-	107	-	139	163	-	-	211
$p^3_{1728}(\ell)$	11	-	23	43	-	-	71	83	-	107	-	-	167	179	-
$p^1_0(\ell)$	-	-	17	-	23	-	53	-	-	89	107	-	113	-	-
$p^2_0(\ell)$	-	11	-	29	-	47	-	53	83	-	-	107	-	137	131
ℓ	59	61	67	71	73	79	83	89	97	101	103	107	109	113	127
$p^1_{1728}(\ell)$	-	239	-	-	283	-	-	347	383	379	-	-	431	443	-
$p^3_{1728}(\ell)$	227	-	263	283	-	311	331	-	-	-	383	419	-	-	503
$p^1_0(\ell)$	-	179	197	-	191	233	-	-	263	-	293	-	311	-	353
$p^2_0(\ell)$	173	-	-	197	-	-	233	263	-	251	-	317	-	311	-
ℓ	131	137	139	149	151	157	163	167	173	179	181	191	193	197	199
$p^1_{1728}(\ell)$	-	547	-	587	-	619	-	-	691	-	719	-	743	787	-
$p^3_{1728}(\ell)$	523	-	547	-	599	-	647	659	-	691	-	751	-	-	787
$p^1_0(\ell)$	-	-	401	-	449	467	461	-	-	-	491	-	563	-	593
$p^2_0(\ell)$	389	383	-	443	-	-	-	449	503	521	-	569	-	587	-
ℓ	211	223	227	229	233	239	241	251	257	263	269	271	277	281	283
$p^1_{1728}(\ell)$	-	-	-	911	919	-	947	-	1019	-	1063	-	1103	1123	-
$p^3_{1728}(\ell)$	839	887	907	-	-	947	-	991	-	1051	-	1039	-	-	1123
$p^1_0(\ell)$	617	653	-	683	-	-	719	-	-	-	-	809	827	-	821
$p^2_0(\ell)$	-	-	677	-	683	701	-	701	743	773	743	-	-	839	-

(i) 当 $\ell \equiv 1 \bmod 4$, $p < 4\ell$ 时, 还是有一些 p 可以使得 E_{1728} 有两条环路. 比如：$\ell = 13$, $p = 31$, E_{1728} 有两条环路.

(ii) 当 $\ell \equiv 3 \bmod 4$, $p < 4\ell$ 时, 还是有一些 p 可以使得 E_{1728} 没有环路. 比如:$\ell = 11$, $p = 23$, E_{1728} 没有环路.

(iii) 当 $\ell \equiv 1 \bmod 3$, $p < 3\ell$, 还是有一些 p 可以使得 E_0 有两条环路比如:$\ell = 13$, $p = 29$, E_0 有两条环路.

(iv) 当 $\ell \equiv 2 \bmod 3$, $p < 3\ell$, 还是有一些 p 可以使得 E_0 没有环路比如:$\ell = 11$, $p = 22$, E_0 没有环路.

(2) 所以我们得到的界是最好的：

(i) 对于 $p \equiv 3 \bmod 4$, $p \geqslant 4\ell$, $\ell \equiv 1 \bmod 4$, 4ℓ 是最小的界使得 E_{1728} 有两条环路. 比如：$\ell = 5$, $4\ell = 20$, $p^1_{1728}(\ell) = 19$ 是最大的 $\equiv 3 \bmod 4$ 的小于 4ℓ 的素数.

(ii) 对于 $p \equiv 3 \bmod 4$, $p \geqslant 4\ell$, $\ell \equiv 3 \bmod 4$, 4ℓ 是最小的界使得 E_{1728} 有没有环路. 比如：$\ell = 7$, $4\ell = 28$, $p^3_{1728}(\ell) = 23$ 是最大的 $\equiv 3 \bmod 4$ 的小

于 4ℓ 的素数.

(iii) 对于 $p \equiv 2 \bmod 3$, $p \geqslant 3\ell$, $\ell \equiv 1 \bmod 3$, 3ℓ 是最小的界使得 E_0 有两条环路. 比如：$\ell = 7$, $3\ell = 21$, $p_0^1(\ell) = 17$ 是最大的 $\equiv 2 \bmod 3$ 的小于 3ℓ 的素数.

(iv) 对于 $p \equiv 2 \bmod 3$, $p \geqslant 3\ell$, $\ell \equiv 2 \bmod 3$, 3ℓ 是最小的界使得 E_0 有没有环路. 比如：$\ell = 5$, $3\ell = 15$, $p_0^2(\ell) = 11$ 是最大的 $\equiv 2 \bmod 3$ 的小于 3ℓ 的素数.

(3) 但是我们给出的界并不是对于每种情况都是最好的：

(i) $p_{1728}^1(\ell)$ 可能不是比 4ℓ 小的最大的 $\equiv 3 \bmod 4$ 的素数. 比如, $\ell = 101$, 最大的 $\equiv 3 \bmod 4$ 小于 4ℓ 的素数是 383, 但 $p_{1728}^1(\ell)$=379.

(ii) $p_{1728}^3(\ell)$ 可能不是比 4ℓ 小的最大的 $\equiv 3 \bmod 4$ 的素数. 比如, $\ell = 271$, 最大的 $\equiv 3 \bmod 4$ 小于 4ℓ 的素数是 1063, 但 $p_{1728}^1(\ell)$=1039.

(iii) $p_0^1(\ell)$ 可能不是比 3ℓ 小的最大的 $\equiv 2 \bmod 3$ 的素数. 比如, $\ell = 193$, 最大的 $\equiv 2 \bmod 3$ 小于 3ℓ 的素数是 569, 但 $p_0^2(\ell)$=563.

(iv) $p_0^2(\ell)$ 可能不是比 3ℓ 小的最大的 $\equiv 2 \bmod 3$ 的素数. 比如, $\ell = 41$, 最大的 $\equiv 2 \bmod 3$ 小于 3ℓ 的素数是 113, 但 $p_0^2(\ell)$=107.

6.2　超奇异椭圆曲线同源图中 $j = 0, 1728$ 邻接的个数

设 $\mathcal{O}$ 为 $B_{p,\infty}$ 的极大序且包含子环 $\mathbb{Z}\langle i, j\rangle$, 其中 $i^2 = -q$, $j^2 = -p$, $ij = -ji$ $((q, p) = 1)$, $K = \mathbb{Q}(i)$. 故当 $q \equiv 1,\ 2 \bmod 4$ 时, 其代数整数环 $\mathcal{O}_K = \mathbb{Z}[i]$, 当 $q \equiv 3 \bmod 4$ 时则为 $\mathbb{Z}[\frac{1+i}{2}]$. 令 $R = \mathcal{O} \bigcap K$. 则 $\mathbb{Z}[i] \subseteq R \subseteq \mathcal{O}_K$. 当 $R = \mathbb{Z}[i]$ 时, 令 $\epsilon = i$; 当 $R = \mathcal{O}_K = \mathbb{Z}[\frac{1+i}{2}]$ 时, 令 $\epsilon = \frac{1+i}{2}$.

由 [13], 令 X_ℓ 为所有的约化范数是 ℓ 的左 $\mathcal{O}$-理想集合. $\hat{r} \in (R/\ell R)^\times$ 且 $r \in R$ 为 $\hat{r}$ 的提升. 则对于任意的 $I \in X_\ell$, $\ell\mathcal{O} + Ir$ 仍在 X_ℓ 中 (通过计算约化范数可以得到), 并且有 $(R/\ell R)^\times$ 在 X_ℓ 上的作用

$$(R/\ell R)^\times \times X_\ell \to X_\ell;\ (\hat{r}, I) \mapsto \mathcal{O}\ell + Ir.$$

定理 6.2　设 $\mathcal{O}, K$ 和 $R = \mathbb{Z}[\epsilon]$ 如上所示. 设 $\ell \nmid 2pq[\mathcal{O} : \mathbb{Z}\langle i, j\rangle]$. 则

(1) 若 ℓ 在 R 中惯性, 则 $(R/\ell R)^\times$ 在 X_ℓ 上的作用是传递的, 此时 $(\mathbb{Z}/\ell\mathbb{Z})^\times$ 为作用的稳定化子.

(2) 若 ℓ 在 R 中分裂, 记为 $\ell R = \mathfrak{p}_1\mathfrak{p}_2$, 则 $\{\mathcal{O}\mathfrak{p}_1, \mathcal{O}\mathfrak{p}_2\} \subset X_\ell$, $(R/\ell R)^\times$ 在 $\mathcal{O}\mathfrak{p}_1$ 和 $\mathcal{O}\mathfrak{p}_2$ 上作用平凡, 且在 $X_\ell - \{\mathcal{O}\mathfrak{p}_1, \mathcal{O}\mathfrak{p}_2\}$ 上作用传递, 此时 $(\mathbb{Z}/\ell\mathbb{Z})^\times$ 为作用的稳定化子.

在这两种情况下, 对于任意的 $I \in X_\ell - \{\mathcal{O}\mathfrak{p}_1, \mathcal{O}\mathfrak{p}_2\}$, $a \in \mathbb{F}_\ell$, 令 $I_a := \ell\mathcal{O} + I(\tilde{a} + \epsilon)$(其中 $\tilde{a} \in \mathbb{Z}$ 为 a 的提升), 则 $X_\ell = \{I, I_a \mid a \in \mathbb{F}_\ell\}$.

证明　由于 $\ell \nmid pq[\mathcal{O} : \mathbb{Z}\langle i, j\rangle]$, 我们有

$$\mathcal{O}/\ell\mathcal{O} = \mathbb{F}_\ell\langle i, j\rangle \ (i^2 = -q,\ j^2 = -p,\ ij = -ji = k).$$

由 [62], 我们得到环同构 $\theta :\ \mathcal{O}/\ell\mathcal{O} \to M_2(\mathbb{F}_\ell)$

$$1 \mapsto \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},\ i \mapsto \begin{pmatrix} 0 & -q \\ 1 & 0 \end{pmatrix},\ j \mapsto \begin{pmatrix} u & qv \\ v & -u \end{pmatrix},$$

其中 $(u,\ v)$ 为 $u^2 + qv^2 = -p$ 在 $\mathbb{F}_\ell$ 中的解 (注意此时方程在 $\mathbb{F}_\ell$ 中可解).

由于 $M_2(\mathbb{F}_\ell)$ 是半单的, 由 [63], 任一非零左理想都是由一个元素生成的, 记生成元为 $M \neq 0$. 由于 M 不是可逆的, 则 $\mathrm{rank}(M) = 1$. 又 $M_2(\mathbb{F}_\ell)M = M_2(\mathbb{F}_\ell)PM$ 对任意的 $P \in \mathrm{GL}_2(\mathbb{F}_\ell)$ 成立. 经计算,

$$\omega := \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix},\ \omega_a := \begin{pmatrix} 1 & a \\ 0 & 0 \end{pmatrix},$$

其中 $a \in \mathbb{F}_\ell$, 生成了 $M_2(\mathbb{F}_\ell)$ 不同的左理想. 从而 $M_2(\mathbb{F}_\ell)$ 所有非零左理想的集合是:

$$\overline{X_\ell} := \{M_2(\mathbb{F}_\ell)\omega, M_2(\mathbb{F}_\ell)\omega_a \mid a \in \mathbb{F}_\ell\}.$$

总之, 通过同构 θ, $\mathcal{O}/\ell\mathcal{O}$ 恰好有 $\ell + 1$ 个左理想, 且都为主理想. 在同态 $\mathcal{O} \to \mathcal{O}/\ell\mathcal{O}$ 下, 集合 X_ℓ 与 $\mathcal{O}/\ell\mathcal{O}$ 的非零左理想一一对应, 因此与 $\overline{X_\ell}$ 一一对应. 进一步, $(R/\ell R)^\times$ 在 X_ℓ 上的作用对应到 $(R/\ell R)^\times$ 在 $\mathcal{O}/\ell\mathcal{O}$ 的非零左理想上的右乘作用, 即对应到 $\theta((R/\ell R)^\times)$ 在 $\overline{X_\ell}$ 上的右乘作用.

像 $\theta((R/\ell R)^\times)$ 中的任一元素有形式 $\begin{pmatrix} x & -qy \\ y & x \end{pmatrix}(x^2 + qy^2 \neq 0)$. 如果 $a_0 \in \mathbb{F}_\ell$ 满足 $a_0^2 + q = 0$, 则 $x + a_0 y \neq 0$ 且

$$\omega_{a_0}\begin{pmatrix} x & -qy \\ y & x \end{pmatrix} = \begin{pmatrix} x + a_0 y & a_0(x + a_0 y) \\ 0 & 0 \end{pmatrix} \in M_2(\mathbb{F}_\ell)\omega_{a_0}.$$

如果 $a \in \mathbb{F}_\ell$ 满足 $a^2 + q \neq 0$, 则对于任意 b 满足 $b^2 + q \neq 0$,

$$\omega_a\begin{pmatrix} \frac{q+ab}{q+a^2} & -q\frac{a-b}{q+a^2} \\ \frac{a-b}{q+a^2} & \frac{q+ab}{q+a^2} \end{pmatrix} = \omega_b, \tag{6.5}$$

且

$$\omega_a\begin{pmatrix} \frac{a}{q+a^2} & q\frac{1}{q+a^2} \\ -\frac{1}{q+a^2} & \frac{a}{q+a^2} \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \in M_2(\mathbb{F}_\ell)\omega. \tag{6.6}$$

由于 $\ell \nmid 2q$, ℓ 与 R 的导子互素且 $R\ell$ 至多为两个 R-理想的乘积.

如果 ℓ 在 R 中惯性, 那么不存在 $a_0 \in \mathbb{F}_\ell$ 使得 ${a_0}^2+q=0$, 即 $\theta((R/\ell R)^\times)$ 在 $\overline{X_\ell}$ 的作用是传递的 (由 (6.5) 和 (6.6) 得到). 在这种情况下, $\{1, a+\epsilon \mid 0 \leqslant a \leqslant \ell-1\}$ 是 $(\mathbb{Z}/\ell\mathbb{Z})^\times$ 在 $(R/\ell R)^\times$ 中的陪集表示, 故 $X_\ell = \{I, I_a \mid a \in \mathbb{F}_\ell\}$, 这里 I 是 X_ℓ 中任意元素.

如果果 ℓ 在 R 中分裂, 即 $\ell R = \mathfrak{p}_1\mathfrak{p}_2$, 那么 $\mathfrak{p}_1 = (\ell, a+\epsilon)$ 且 $\mathfrak{p}_2 = \bar{\mathfrak{p}}_1 = (\ell, a+\bar{\epsilon})$, $a \in \mathbb{Z}$ 使得 $\mathrm{N}(a+\epsilon) = \mathrm{Nrd}(a+\epsilon) = 0 \in \mathbb{F}_\ell$, 这说明 $\mathcal{O}\mathfrak{p}_1 = \ell\mathcal{O} + \mathcal{O}(a+\epsilon)$ 且 $\mathcal{O}\mathfrak{p}_2 = \ell\mathcal{O} + \mathcal{O}(a+\bar{\epsilon})$ 在 X_ℓ 中. 也说明了存在 $a_0 \in \mathbb{F}_\ell$ 使得 ${a_0}^2 + q = 0$. 因此 $\theta((R/\ell R)^\times)$ 有一个长为 $\ell-1$ 的轨道和两个固定点 $\omega_{a_0}, \omega_{-a_0}$. 在这种情况下, $\{1, b+\epsilon \mid b \in \mathbb{F}_\ell, N(b+\epsilon) \neq 0\}$ 为 $(\mathbb{Z}/\ell\mathbb{Z})^\times$ 在 $(R/\ell R)^\times$ 中的陪集表示. 由

$$I = \mathcal{O}\mathfrak{p}_1 = \ell\mathcal{O} + \mathcal{O}(a+\epsilon) \quad \text{或} \qquad I = \mathcal{O}\mathfrak{p}_2,$$

$$\ell\mathcal{O} + Ir = \ell\mathcal{O} + rI \subseteq I,$$

则

$$\ell\mathcal{O} + Ir = I,$$

由于它们都为左 $\mathcal{O}$-理想且约化范数是 ℓ. 因此对于任意的 $I \in X_\ell - \{\mathcal{O}\mathfrak{p}_1, \mathcal{O}\mathfrak{p}_2\}$, 我们仍有 $X_\ell = \{I, I_a \mid a \in \mathbb{F}_\ell\}$. □

注　对于任意的 $I \in X_\ell$, 从证明中可以看出,

$$I = \mathcal{O}\ell + \mathcal{O}\alpha \qquad (\alpha \in \mathcal{O}).$$

我们将用上面的定理来证明邻接个数结果, 设 I 为 $\mathrm{End}(E_0)$ 或者 $\mathrm{End}(E_{1728})$ 的一个约化范数是 ℓ 的左理想, X_ℓ 为 $\{I,\ I_a \mid a \in \mathbb{F}_\ell\}$. 我们将通过计算, 将理想按照理想类分类, 应用 Deuring 对应定理 2.27, 得到 $[E_0]$ 和 $[E_{1728}]$ 的边和邻接的信息.

6.2.1　$j = 1728$ 邻接的个数

此时 E_{1728} 的自同态环是 $\mathcal{O}_{1728}$, $R = \mathcal{O}_{1728} \cap \mathbb{Q}(i) = \mathbb{Z}[i]$ 为主理想整环, 它的单位群是 $\{\pm 1, \pm i\}$.

我们需要一些引理：

引理 6.3　设 $\ell \equiv 1 \bmod 4$.

(1) 若 ℓ 在 $\mathbb{Z}[i]$ 中完全分裂,

$$\ell\mathbb{Z}[i] = (m+ni)\mathbb{Z}[i] \cdot (m-ni)\mathbb{Z}[i],$$

其中 $(m,n) \in \mathbb{Z}^2$ 为 $X^2+Y^2=\ell$ 的解. 则 $X^2+Y^2=\ell$ 的解为

$$\{(\pm m, \pm n), (\pm n, \pm m)\}.$$

(2) 由 (1), 对于 $(x,y)\in\mathbb{Z}^2$ 满足 $\ell\nmid x$ 且 $X^2+Y^2=\ell^2$ 的解为

$$\{(\pm(m^2-n^2),\pm 2mn),(\pm 2mn,\pm(m^2-n^2))\}.$$

(3) 左 $\mathcal{O}$-理想 $\mathcal{O}(m+ni)$ 和 $\mathcal{O}(m-ni)$ 约化范数为 ℓ. 进一步, 对于任意的约化范数为 ℓ 的左 $\mathcal{O}$ 理想 J, 令 $b=m/n\in\mathbb{F}_\ell$, 则 $b^2=-1$,

$$J_b=\ell\mathcal{O}+J(\tilde{b}+i)=\ell\mathcal{O}+J(m+ni)=\mathcal{O}(m+ni),\qquad J_{-b}=\mathcal{O}(m-ni).$$

证明　参考 [23] 引理 8. □

引理 6.4　设 $p>4\ell^2$. 若 $\mu\in\ell^{-1}\mathcal{O}$, $\mathrm{Nrd}(\mu)=1$, $\mu\notin\{\pm 1,\pm i\}$, 则 $\ell\equiv 1 \bmod 4$ 且 $\mu=\ell^{-1}(x+yi)$, 其中 $(x,y)\in\mathbb{Z}^2$ 满足 $\ell\nmid x$, $X^2+Y^2=\ell^2$.

证明　记

$$\mu=\frac{1}{\ell}\Big(A+Bi+C\frac{1+j}{2}+D\frac{i+k}{2}\Big),\quad (A,B,C,D\in\mathbb{Z}).$$

由于 $\mathrm{Nrd}(\mu)=1$, 则

$$\Big(A+\frac{C}{2}\Big)^2+\Big(B+\frac{D}{2}\Big)^2+\frac{p(C^2+D^2)}{4}=\ell^2.$$

若 $p>4\ell^2$, 则 $C=D=0$, 从而 $\mu=\frac{A+Bi}{\ell}$, $A^2+B^2=\ell^2$. 若 $\ell\mid A$, 则 $\ell\mid B$, $\mu\in\{\pm 1,\pm i\}$. 若 $\ell\nmid A$, 则 $(B/A)^2=-1\in\mathbb{F}_\ell$, $\ell\equiv 1 \bmod 4$. □

定理 6.5　[23] 设 $\ell>3$. 若 $p\equiv 3 \bmod 4$ 且 $p>4\ell^2$, 则 $[E_{1728}]$ 在图中存在 $\frac{1}{2}\big(\ell-(-1)^{\frac{\ell-1}{2}}\big)$ 个邻接, 通过两条边连接 $[E_{1728}]$ 的每个顶点 ($[E_{1728}]$ 除外).

证明　若 $\ell\equiv 1 \bmod 4$, 令 $(m,n)\in\mathbb{Z}^2$ 为 $x^2+y^2=\ell$ 的解且 $b=mn^{-1}\in\mathbb{F}_\ell$, 故此时 $b^2=-1$.

设 I 为约化范数为 ℓ 的左 $\mathcal{O}$-理想, 且不为 $\mathcal{O}(m\pm ni)$(若 $\ell\equiv 1 \bmod 4$). 通过定理 6.2, 所有约化范数是 ℓ 的 $\ell+1$ 个左 $\mathcal{O}$-理想的集合为:

$$X_\ell=\{I,\ I_a=\ell\mathcal{O}+I(a+i)\mid a\in\mathbb{F}_\ell=\{0,\cdots,\ell-1\}\}.$$

若 $\ell\equiv 1 \bmod 4$, 通过引理 6.3, 设 $I_b=\mathcal{O}(m+ni)$ 且 $I_{-b}=\mathcal{O}(m-ni)$.

我们断言

$$Ii=I_0,\qquad I_0i=I,\qquad I_ai=I_{-a^{-1}}\qquad (a\neq 0).$$

事实上, 由引理 2.26可知 $\ell\in I$, 则 $\ell i\in I$, $\ell=-\ell ii\in Ii$, 因此

$$I_0=Ii+\ell\mathcal{O}=Ii,\qquad I=I_0i.$$

由在 $\mathbb{F}_\ell$ 中 $a \neq 0, i \in \mathcal{O}$ 则 $\ell\mathcal{O}i \subseteq \ell\mathcal{O}$, 且 $I_a i$ 为左 $\mathcal{O}$-理想, $\ell\mathcal{O} \subseteq I_a i$. 因此

$$I_a i = \ell\mathcal{O}i + I(-1 + ai) = \ell\mathcal{O} + \ell\mathcal{O}i + I(-a^{-1} + i) = \ell\mathcal{O} + I(-a^{-1} + i) = I_{-a^{-1}}.$$

综上, 我们将 X_ℓ 分为 $\frac{\ell+1}{2}$ 个子集, 每个子集有 2 个元素在同一个理想类:

$$\{I, I_0\}, \qquad \{I_a, I_{-a^{-1}}\}(a^2 \neq 0, -1), \qquad \{I_b, I_{-b}\}(b^2 = -1).$$

我们将证明在不同子集中的理想不在同一个理想等价类中.

设 I 和 J 是在 X_ℓ 的不同子集中且 $I = J\mu(\mu \in B_{p,\infty})$, 则 $\mu \notin \{\pm 1, \pm i\}$ 且 $\mathrm{Nrd}(\mu) = 1$. 由于

$$\ell \in J, \qquad \ell\mu \in I \subseteq \mathcal{O}, \qquad \mu \in \ell^{-1}\mathcal{O}.$$

通过引理 6.4, 我们有

$$\ell \equiv 1 \bmod 4, \qquad \mu = \frac{A + Bi}{\ell}, \qquad A^2 + B^2 = \ell^2, \qquad \ell \nmid A.$$

这说明

$$A + Bi = u(m \pm ni)^2 (u \in \{\pm 1, \pm i\}),$$

因此 $\gcd(A + Bi, \ell)$ 在 $\mathbb{Z}[i]$ 中为 $u(m \pm ni)$.

特别地, $I_{\pm b} = \mathcal{O}(m + ni) \subseteq I$, 因此由其有相同的约化范数, 则 $I_{\pm b} = I$. 将 I 换成 J, 我们可以得到 $J = I_{\pm b}$. 因此 I 和 J 在同一个子集 $\{I_b, I_{-b}\}$ 中, 这是不可能的. 由 Deuring 定理 2.27和定理 6.1, 当 $\ell \equiv 3 \bmod 4$ 时, 没有子集对应这些自同态. 即证. □

6.2.2　$j = 0$ 邻接的个数

此由 E_0 的自同态环是 $\mathcal{O}_0$, $R = \mathcal{O}_0 \cap \mathbb{Q}(i) = \mathbb{Z}[\epsilon](\epsilon = \frac{1+i}{2})$ 为主理想整环, 它的单位群是 $\{\pm 1, \pm\epsilon, \pm\bar{\epsilon}\}$.

我们需要一些引理：

引理 6.6　设 $\ell \equiv 1 \bmod 3$.

(1) 若 ℓ 在 $\mathbb{Z}[\epsilon]$ 中完全分裂,

$$\ell\mathbb{Z}[\epsilon] = (m + n\epsilon)\mathbb{Z}[\epsilon] \cdot (m + n\bar{\epsilon})\mathbb{Z}[\epsilon],$$

其中 $(m, n) \in \mathbb{Z}^2$ 为 $X^2 + XY + Y^2 = \ell$ 的解. 则 $X^2 + XY + Y^2 = \ell$ 的解为

$$\{\pm(m, n), \pm(n, m), \pm(m + n, -n), \pm(m + n, -m), \pm(-n, m + n), \pm(-m, m + n)\}.$$

(2) 由 (1), 对于 $(x, y) \in \mathbb{Z}^2$ 满足 $\ell \nmid x$ 且 $X^2 + XY + Y^2 = \ell^2$ 的解为

$$\{\pm((m^2 - n^2), n^2 + 2mn), (\pm(n^2 - m^2), \pm(m^2 + 2mn)), \pm((m^2 + 2mn), -(n^2 + 2mn)),$$

$$\pm((n^2 + 2mn), -(m^2 + 2mn)), \pm((m^2 + 2mn), n^2 - m^2), \pm((n^2 + 2mn), m^2 - n^2)\}.$$

(3) 左 $\mathcal{O}$-理想 $\mathcal{O}(m+n\epsilon)$, $\mathcal{O}(m+n\bar{\epsilon})$ 的约化范数为 ℓ. 进一步, 对于任意的约化范数为 ℓ 的左 $\mathcal{O}$ 理想, 令 $b=m/n\in\mathbb{F}_\ell$, 则 $b^2+b+1=0$,

$$J_b=\ell\mathcal{O}+J(\tilde{b}+\epsilon)=\ell\mathcal{O}+J(m+n\epsilon)=\mathcal{O}(m+n\epsilon),\qquad J_{b^2}=\mathcal{O}(m+n\bar{\epsilon}).$$

证明　参考 [23] 引理 10. □

引理 6.7　设 $p>3\ell^2$. 若 $\mu\in\ell^{-1}\mathcal{O}$, $\mathrm{Nrd}(\mu)=1$ 且 $\mu\notin\{\pm1,\pm\epsilon,\pm\bar{\epsilon}\}$, 则 $\ell\equiv1 \bmod 3$ 且 $\mu=\ell^{-1}(x+y\epsilon)$, 其中 $(x,y)\in\mathbb{Z}^2$ 满足 $\ell\nmid x$ and $X^2+XY+Y^2=\ell^2$.

证明　记

$$\mu=\frac{1}{\ell}\Big(A+B\frac{1+i}{2}+C\frac{i+k}{3}+D\frac{j+k}{2}\Big),\quad (A,B,C,D\in\mathbb{Z}).$$

由于 $\mathrm{Nrd}(\mu)=1$, 则

$$\Big(A+\frac{B}{2}\Big)^2+3\Big(\frac{B}{2}+\frac{C}{3}\Big)^2+\frac{p}{3}(C^2+3CD+3D^2)=\ell^2.$$

若 $p>3\ell^2$, 则 $C=D=0$, 从而 $\mu=\frac{A+B\frac{1+i}{2}}{\ell}$, $A^2+AB+B^2=\ell^2$. 若 $\ell\mid A$, 则 $\ell\mid B$, $\mu\in\{\pm1,\pm\frac{1+i}{2},\pm\frac{1-i}{2}\}$. 若 $\ell\nmid A$, 则 $(B/A)^2+(B/A)+1=0\in\mathbb{F}_\ell$, $\ell\equiv1 \bmod 3$. □

定理 6.8　[23] 设 $\ell>3$. 如果 $p\equiv2 \bmod 3$ 且 $p>3\ell^2$, 则 $[E_0]$ 在图中存在 $\frac{1}{3}(\ell-(\frac{\ell}{3}))$ 个邻接, 通过三条边连接 $[E_0]$ 的每个顶点 ($[E_0]$ 除外).

证明　若 $\ell\equiv1 \bmod 3$, 令 $(m,n)\in\mathbb{Z}^2$ 为 $x^2+xy+y^2=\ell$ 的解且 $b=mn^{-1}\in\mathbb{F}_\ell$, 故此时 $b^2+b+1=0$.

对于 I 为约化范数为 ℓ 的左 $\mathcal{O}$-理想, 且不为 $\mathcal{O}(m+n\epsilon)$, $\mathcal{O}(m+n\bar{\epsilon})$ (若 $\ell\equiv1 \bmod 3$). 通过定理 6.2, 所有约化范数是 ℓ 的, $\ell+1$ 个左 $\mathcal{O}$-理想的集合为:

$$X_\ell=\{I,\ I_a=\ell\mathcal{O}+I(a+\frac{1+i}{2})\mid a\in\mathbb{F}_\ell=\{0,\cdots,\ell-1\}\}.$$

若 $\ell\equiv1 \bmod 3$, 通过引理 6.6, 令 $I_b=\mathcal{O}(m+n\epsilon)$ 且 $I_{b^2}=\mathcal{O}(m+n\bar{\epsilon})$.

我们断言

$$I\epsilon=I_0,\qquad I\bar{\epsilon}=I_{-1}\qquad I_a\epsilon=I_{-(a+1)^{-1}},\qquad I_a\bar{\epsilon}=I_{-a^{-1}(a+1)}\qquad (a\neq0,-1).$$

事实上, 由引理 2.26可知 $\ell\in I$. 则 $\ell,\ell\bar{\epsilon}\in I$, $\ell=\ell\bar{\epsilon}\epsilon\in I\epsilon$, 因此

$$I_0=I\epsilon+\ell\mathcal{O}=I\epsilon,\qquad I\bar{\epsilon}=I_{-1}.$$

由于在 $\mathbb{F}_\ell$ 中 $a\neq0,-1$, $\epsilon\in\mathcal{O}$, 则 $\ell\mathcal{O}\epsilon\subseteq\ell\mathcal{O}$, 且 $I_a\epsilon$ 为左-$\mathcal{O}$ 理想, $\ell\mathcal{O}\subseteq I_a\epsilon$(同样的 $\ell\mathcal{O}\subseteq I_a\bar{\epsilon}$) . 因此

$$\begin{aligned}I_a\epsilon&=\ell\mathcal{O}\epsilon+I(-1+(a+1)\epsilon)=\ell\mathcal{O}+\ell\mathcal{O}\epsilon+I(-1+(a+1)\epsilon)\\&=\ell\mathcal{O}+I(-1+(a+1)\epsilon)=\ell\mathcal{O}+I(-(a+1)^{-1}+\epsilon)\\&=I_{-(a+1)^{-1}},\end{aligned}$$

$$\begin{aligned} I_a\bar{\epsilon} &= \ell\mathcal{O}\bar{\epsilon} + I((a+1) - a\epsilon) = \ell\mathcal{O} + \ell\mathcal{O}\bar{\epsilon} + I((a+1) - a\epsilon) \\ &= \ell\mathcal{O} + I((a+1) - a\epsilon) = \ell\mathcal{O} + I(-(a+1)a^{-1} + \epsilon) \\ &= I_{-a^{-1}(a+1)}, \end{aligned}$$

.

综上, 我们将 X_ℓ 分为 $[\frac{\ell+2}{3}]$ 个子集, 每一个子集包含 2 或者 3 个元素在同一个理想类:

$$\{I, I_0, I_{-1}\}, \qquad \{I_a, I_{-(a+1)^{-1}}, I_{-a^{-1}(a+1)}\}(a^2+a+1 \neq 0, 1), \qquad \{I_b, I_{b^2}\}(b^2+b+1 = 0).$$

我们将证明在不同子集中的理想不在同一个理想等价类中.

设 I 和 J 是在 X_ℓ 的不同子集中且 $I = J\mu$ ($\mu \in B_{p,\infty}$), 则 $\mu \notin \{\pm 1, \pm\epsilon, \pm\bar{\epsilon}\}$ 且 $\mathrm{Nrd}(\mu) = 1$. 由于

$$\ell \in J, \qquad \ell\mu \in I \subseteq \mathcal{O}, \qquad \mu \in \ell^{-1}\mathcal{O}.$$

通过引理 6.7, 我们有

$$\ell \equiv 1 \bmod 3, \qquad \mu = \frac{A + B\epsilon}{\ell}, \qquad A^2 + AB + B^2 = \ell^2, \qquad \ell \nmid A.$$

这说明

$$A + B\epsilon = u(m + n\frac{1 \pm i}{2})^2 (u \in \{\pm 1, \pm\epsilon, \pm\bar{\epsilon}\}),$$

因此 $\gcd(A + B\epsilon, \ell)$ 在 $\mathbb{Z}[\frac{1+\sqrt{-3}}{2}]$ 中为 $u(m + n\frac{1\pm i}{2})$.

特别地, $I_b = \mathcal{O}(m + n\epsilon) \subseteq I$ 或者 $I_{b^2} = \mathcal{O}(m + n\bar{\epsilon}) \subseteq I$, 因此由其有相同的约化范数, 则 $I_b = I$ 或者 $I_{b^2} = I$. 将 I 换成 J, 我们可以得到 $J = I_b$ 或者 $J = I_{b^2}$. 因此 I 和 J 在同一个子集 $\{I_b, I_{b^2}\}$, 这是不可能的. 由 Deuring 2.27定理和定理6.1, 当 $\ell \equiv 2 \bmod 3$ 时, 没有子集对应这些自同态. □

6.2.3　E_{1728} 的 $\mathbb{F}_p$ 同源的个数

引理 6.9　设 $p > 4\ell^2$. 若 $s \in \ell^{-1}\mathcal{O}$, $s^2 = -p$, $s \notin \{\pm j, \pm k\}$, 则 $\ell \equiv 1 \bmod 4$, 且 $s = \ell^{-1}(xj + yk)$, 其中 $(x, y) \in \mathbb{Z}^2$ 满足 $\ell \nmid x$, $X^2 + Y^2 = \ell^2$.

证明　记

$$s = \ell^{-1}(a + bi + c\frac{1 + j}{2} + d\frac{i + k}{2}).$$

则 $s^2 = -p \in \mathbb{Q}$ 推出 $a + \frac{c}{2} = 0$, $c \in 2\mathbb{Z}$. 进一步,

$$\ell^2 p = -\ell^2 s^2 = \mathrm{Nrd}(\ell s) = \left(b + \frac{d}{2}\right)^2 + \frac{p}{4}(c^2 + d^2)$$

推出 $p \mid 2b + d$. 若 $2b + d \neq 0$, 则 $(b + \frac{d}{2})^2 \geqslant \frac{p^2}{4} > p\ell^2$ (由于 $p > 4\ell^2$), 这是不可能的. 从而 $b + \frac{d}{2} = 0$, $d \in 2\mathbb{Z}$. 因此 $s \in \ell^{-1}\mathcal{O}(s^2 = -p)$ 有形式

$$s = \ell^{-1}(xj + yk),$$

其中 $x, y \in \mathbb{Z}$, $x^2 + y^2 = \ell^2$.

若 $\ell \mid x$, 则 $\ell \mid y$. 这说明

$$s = Xj + Yk \qquad (X, Y \in \mathbb{Z}),$$

又由 $\mathrm{Nrd}(Xj + Yk) = (X^2 + Y^2)p$, 则 $-p$ 在 $\mathbb{Z}[j, k]$ 中的平方根为 $\{\pm j, \pm k\}$. 由此可得

$$s \in \{\pm j, \pm k\}.$$

否则我们仍有 $(y/x)^2 = -1 \in \mathbb{F}_\ell$, $\ell \equiv 1 \bmod 4$. □

定理 6.10 [23] 对于 $j = 1728$, $p > 4\ell^2$ 时, 有 $1 + (\frac{\ell}{p})$ 个与其相连的顶点的 j-不变量落在 $\mathbb{F}_p - \{1728\}$ 中.

证明　设 E 为定义在 $\mathbb{F}_p$ 上的超奇异椭圆曲线且, E_{1728} 通过约化范数为 ℓ 的左 $\mathcal{O}$-理想连接到 E. 通过定理 4.5, 超奇异椭圆曲线定义在 $\mathbb{F}_p$ 上当且仅当 $\mathbb{Z}[\sqrt{-p}]$ 在其自同态环中. 则 $\mathrm{End}(E) = \mathcal{O}_R(I) \subseteq \ell^{-1}\mathcal{O}$ 有元素 s 满足 $s^2 = -p$. 由引理 6.9, 我们知道

$$s \in \{\pm j, \pm k\}$$

或者当 $\ell \equiv 1 \bmod 4$ 时,

$$\ell s = xj + yk \qquad ((x, y) \in \mathbb{Z}^2)$$

使得 $\ell \nmid x$, $x^2 + y^2 = \ell^2$.

令 $\hat{\mathcal{O}} = \mathcal{O}/\ell\mathcal{O}$. 则 $\hat{\mathcal{O}}$ 为 $\mathbb{F}_\ell$ 上的四元数代数. 我们通过 $q = 1$ 时定理 6.2中的同构 θ 将 $\hat{\mathcal{O}}$ 与 $M_2(\mathbb{F}_\ell)$ 对应起来. 进一步, 定理 6.2 中定义的 $\overline{X_\ell}$ 一一对应一一对应到 X_ℓ. 令 I_a 为约化范数为 ℓ 的左 $\mathcal{O}$-理想对应到 $\hat{I}_a = M_2(\mathbb{F}_\ell)\omega_a$ 在 $\overline{X}_\ell$ 中. 对于 $s \in \mathcal{O}$, 令 $\hat{s}$ 为 s 在 $M_2(\mathbb{F}_\ell)$ 中的像. 此时记 i, j, k 为 $\hat{i}, \hat{j}, \hat{k}$.

若 $(\frac{-p}{\ell}) = 1$, 令 $t \in \mathbb{F}_\ell$ 使得 $t^2 = -p$ 且令 $(u, v) = (t, 0)$. 此时,

$$I_\infty = \mathcal{O}\ell + \mathcal{O}(-t + j), \qquad I_a = \mathcal{O}\ell + \mathcal{O}(-t + j)(a + i).$$

则有

$$\hat{I}_\infty j \subset \hat{I}_\infty, \qquad \hat{I}_0 j \subset \hat{I}_0, \qquad \hat{I}_a j \nsubseteq \hat{I}_a \qquad (\text{对于任意的 } a \text{ 都成立}),$$

这说明

$$j \in \mathcal{O}_R(I_\infty), \qquad j \in \mathcal{O}_R(I_0), \qquad j \notin \mathcal{O}_R(I_a) \qquad (\text{对其他的 } a \text{ 成立}).$$

同样的,

$$k \in \mathcal{O}_R(I_{\pm 1}), \qquad k \notin \mathcal{O}_R(I_a) \qquad (\text{对其他的 } a \text{ 成立}).$$

则当 $\ell \equiv 1 \bmod 4$, (x, y) 为 $x^2 + y^2 = \ell^2$ 任意解且 $\ell \nmid x$ 时, 可以验证

$$\hat{I}_a(\hat{x}j + \hat{y}k) \neq 0 \qquad (a^2 \neq -1),$$

因此

$$\mathcal{O}(xj + yk) \subsetneq \ell\mathcal{O}, \qquad \ell^{-1}(xj + yk) \notin O_R(I_a) \qquad (a^2 \neq -1).$$

若 $a^2 = -1$, 则

$$I_a = \mathcal{O}(m + ni) \qquad \text{或者} \qquad I_a = \mathcal{O}(m - ni) \qquad (m^2 + n^2 = \ell),$$

对应到环路. 总之, 有两个定义在 $\mathbb{F}_p$ 的顶点连接到 $[E_{1728}]$, 一个对应理想 $[I_\infty] = [I_0]$, 另一个则对应理想 $[I_1] = [I_{-1}]$.

若 $(\frac{-p}{\ell}) = -1$, 则对于 (u, v) 为 $X^2+Y^2 = -p$ 的任意解有 $uv \neq 0$. 从而 $\omega j \notin \hat{I}_\infty$. 由 $a \in \mathbb{F}_\ell$, $\omega_a j \in \hat{I}_a$ 可以推出 $2au = (1 - a^2)v$. 而 $uv \neq 0$, 则 $a \neq 0, \pm 1$, $v = \frac{2a}{1-a^2}u$. 因此 $-p = \frac{(1+a^2)^2}{(1-a^2)^2}u^2$, 这是不可能的. 这说明 $j \notin I_a$ (对任意的 $a \in \mathbb{F}_\ell \cup \{\infty\}$). 同样的, $k \notin I_a$ (对任意的 $a \in \mathbb{F}_\ell \cup \{\infty\}$). 若 $x, y \neq 0$ 使得 $\omega_a(x + yi)j = 0$, 通过计算得, $a^2 + 1 = 0$, 对应到环路. 总之, 除了自己没有定义在 $\mathbb{F}_p$ 上的顶点连接 $[E_{1728}]$. □

6.2.4　E_0 的 $\mathbb{F}_p$ 同源的个数

引理 6.11　设 $p > 3\ell^2$. 若 $s \in \ell^{-1}\mathcal{O}$, $s^2 = -p$, $s \notin \{\pm j, \pm\epsilon j, \pm\bar{\epsilon} j\}$, 则 $\ell \equiv 1 \bmod 3$, 且 $s = \ell^{-1}(x + y\epsilon)j$, 其中 $(x, y) \in \mathbb{Z}^2$ 满足 $\ell \nmid x$, $X^2 + XY + Y^2 = \ell^2$.

证明　记

$$s = \ell^{-1}(a + b\frac{1 + i}{2} + c\frac{i + k}{3} + d\frac{j + k}{2}).$$

则 $s^2 = -p \in \mathbb{Q}$ 推出 $a + \frac{b}{2} = 0$, $b \in 2\mathbb{Z}$. 进一步,

$$\ell^2 p = -\ell^2 s^2 = \mathrm{Nrd}(\ell s) = 3\left(\frac{b}{2} + \frac{c}{3}\right)^2 + \frac{p}{3}(c^2 + 3cd + 3d^2)$$

推出 $p \mid \frac{3}{2}b + c$. 若 $\frac{3}{2}b + c \neq 0$, 则 $3(\frac{b}{2} + \frac{c}{3})^2 \geqslant \frac{p^2}{3} > p\ell^2$ (由于 $p > 3\ell^2$), 这是不可能的. 从而 $\frac{3}{2}b + c = 0$, $c \in 3\mathbb{Z}$. 因此 $s \in \ell^{-1}\mathcal{O}(s^2 = -p)$ 有形式

$$s = \ell^{-1}(x + y\frac{1 + i}{2})j,$$

其中 $x, y \in \mathbb{Z}$, $x^2 + xy + y^2 = \ell^2$.

若 $\ell \mid x$, 则 $\ell \mid y$. 这说明

$$s = (X + Y\frac{1 + i}{2})j \qquad (X, Y \in \mathbb{Z}),$$

又由 $\mathrm{Nrd}((X+Y\frac{1+i}{2})j) = (X^2+XY+Y^2)p$, 则 $-p$ 在 $\mathbb{Z}[j, \frac{1+i}{2}j]$ 中的平方根为 $\{\pm j, \pm\frac{1+i}{2}j, \pm\frac{1-i}{2}j\}$. 由此可得

$$s \in \{\pm j, \pm\frac{1+i}{2}j, \pm\frac{1-i}{2}j\}.$$

否则我们仍有 $(y/x)^2 + (y/x) + 1 = 0 \in \mathbb{F}_\ell$, $\ell \equiv 1 \bmod 3$. □

定理 6.12 [23] 对于 $j = 0$, $p > 3\ell^2$ 时, 有 $1 + (\frac{-p}{\ell})$ 个与其相连的顶点的 j-不变量落在 $\mathbb{F}_p^*$ 中.

证明　设 E 为定义在 $\mathbb{F}_p$ 上的超奇异椭圆曲线且 E_0 通过约化范数为 ℓ 的左 $\mathcal{O}$-理想连接到 E. 通过定理 4.5, 超奇异椭圆曲线定义在 $\mathbb{F}_p$ 上当且仅当 $\mathbb{Z}[\sqrt{-p}]$ 在其自同态环中. 则 $\mathrm{End}(E) = \mathcal{O}_R(I) \subseteq \ell^{-1}\mathcal{O}$ 有元素 s 满足 $s^2 = -p$. 由引理 6.11, 我们知道

$$s \in \{\pm j, \pm\epsilon j, \pm\bar{\epsilon} j\}$$

或者当 $\ell \equiv 1 \bmod 3$ 时,

$$\ell s = xj + y\epsilon j, \qquad ((x, y) \in \mathbb{Z}^2)$$

使得 $\ell \nmid x$, $x^2 + +xy + y^2 = \ell^2$.

令 $\hat{\mathcal{O}} = \mathcal{O}/\ell\mathcal{O}$. 则 $\hat{\mathcal{O}}$ 为 $\mathbb{F}_\ell$ 上的四元数代数. 我们通过 $q = 3$ 时定理 6.2中的同构 θ 将 $\hat{\mathcal{O}}$ 与 $M_2(\mathbb{F}_\ell)$ 对应起来. 进一步, 定理 6.2 中定义的 $\overline{X_\ell}$ 一一对应一一对应到 X_ℓ. 进一步,

$$\overline{X}_\ell = \{\hat{I}_\infty = M_2(\mathbb{F}_\ell)\begin{pmatrix}0 & 0\\ 0 & 1\end{pmatrix},\ \hat{I}_a := M_2(\mathbb{F}_\ell)\begin{pmatrix}1 & 2a+1\\ 0 & 0\end{pmatrix}\ (a \in \mathbb{F}_\ell)\}$$

一一对应到 X_ℓ. 为了方便, 、$\overline{X_\ell}$ 在这里的形式与证明定理 6.2中的不同. 令 I_a 为约化范数为 ℓ 的左 $\mathcal{O}$-理想对应到 $\hat{I}_a$. 对于 $s \in \mathcal{O}$, 令 $\hat{s}$ 为 s 在 $M_2(\mathbb{F}_\ell)$ 中的像. 此时记 i, j, k 为 $\hat{i}, \hat{j}, \hat{k}$.

若 $(\frac{-p}{\ell}) = 1$, 令 $t \in \mathbb{F}_\ell$ 使得 $t^2 = -p$ 且令 $(u, v) = (t, 0)$. 此时,

$$I_\infty = \mathcal{O}\ell + \mathcal{O}(-t + j), \qquad I_a = \mathcal{O}\ell + \mathcal{O}(-t + j)(a + \epsilon).$$

则有

$$\hat{I}_\infty j \subset \hat{I}_\infty, \qquad \hat{I}_{-2^{-1}} j \subset \hat{I}_{-2^{-1}}, \qquad \hat{I}_a j \nsubseteq \hat{I}_a \qquad \text{(对于任意的 } a \text{ 都成立)},$$

这说明

$$j \in \mathcal{O}_R(I_\infty), \qquad j \in \mathcal{O}_R(I_{-2^{-1}}) \qquad j \notin \mathcal{O}_R(I_a) \qquad \text{(对于其他的 } a\text{)}.$$

同样的,

$$\epsilon j \in \mathcal{O}_R(I_0), \mathcal{O}_R(I_{-2}), \qquad \epsilon j \notin \mathcal{O}_R(I_a)$$

且

$$\bar{\epsilon} j \in \mathcal{O}_R(I_{-1}), \mathcal{O}_R(I_1), \qquad \bar{\epsilon} j \notin \mathcal{O}_R(I_a) \qquad (\text{对其他的 } a).$$

则当 $\ell \equiv 1 \bmod 3$, (x, y) 为 $x^2 + xy + y^2 = \ell^2$ 的任意解且 $\ell \nmid x$ 时, 可以验证

$$\hat{I}_a(\hat{x} j + \hat{y} \epsilon j) \neq 0 \qquad (a^2 + a + 1 \neq 0),$$

因此

$$\mathcal{O}(xj + y\epsilon j) \subsetneq \ell\mathcal{O}, \qquad \ell^{-1}(xj + y\epsilon j) \notin O_R(I_a) \qquad (a^2 + a + 1 \neq 0).$$

若 $a^2 + a + 1 = 0$, 则

$$I_a = \mathcal{O}(m + n\epsilon) \qquad \text{或者} \qquad I_a = (m + n\bar{\epsilon}) \qquad (m^2 + mn + n^2 = \ell),$$

对应到环路. 总之, 有两个定义在 $\mathbb{F}_p$ 的顶点连接到 $[E_0]$, 一个对应理想 $[I_\infty] = [I_0] = [I_{-1}]$, 另一个则对应理想 $[I_1] = [I_{-2^{-1}}] = [I_{-2}]$.

若 $(\frac{-p}{\ell}) = -1$, 则对于 (u, v) 为 $X^2 + 3Y^2 = -p$ 的任意解有 $uv \neq 0$. 从而

$$\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} j \notin \hat{I}_\infty.$$

对于 $a \in \mathbb{F}_\ell$, $\begin{pmatrix} 1 & a \\ 0 & 0 \end{pmatrix} j \in \hat{I}_a$ 可以推出

$$2(2a + 1)u = (3 - (2a + 1)^2)v.$$

又由 $v \neq 0$, 则

$$2a + 1 \neq 0, \qquad u = \frac{3 - (2a + 1)^2}{2(2a + 1)} v.$$

因此 $-p = \frac{(3+(2a+1)^2)^2}{(2(2a+1))^2} v^2$, 这是不可能的. 这说明 $j \notin I_a$(对于任意的 $a \in \mathbb{F}_\ell \cup \{\infty\}$). 同样的, $\epsilon j, \bar{\epsilon} j \notin I_a$ (对于任意的 $a \in \mathbb{F}_\ell \cup \{\infty\}$). 若 $x, y \neq 0$ 使得

$$\begin{pmatrix} 1 & 2a + 1 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 2x + y & -3y \\ y & 2x + y \end{pmatrix} \begin{pmatrix} u & 3v \\ v & -u \end{pmatrix} = 0,$$

通过计算得, $a^2 + a + 1 = 0$, 对应到环路. 总之, 除了自己没有定义在 $\mathbb{F}_p$ 上的顶点连接 $[E_0]$. □

由命题 2.19, 连接 $E_0(E_{1728})$ 的超奇异椭圆曲线的 j-不变量为 $\Phi_\ell(0, X)$ ($\Phi_\ell(1728, X)$) 的根, 从而我们的结果可以写成关于模多项式根的形式.

定理 6.13　设 $\ell > 3$.

(1) 若 $p \equiv 3 \bmod 4$ 且 $p > 4\ell^2$, 则当 $\ell \equiv 3 \bmod 4$ 时,

$$\Phi_\ell(1728, X) = \prod_{i=1}^{(\ell+1)/2} (X - a_i)^2,$$

且有 $1 + (\frac{\ell}{p})$ 个根 $a_i \in \mathbb{F}_p - \{1728\}$, 剩下的在 $\mathbb{F}_{p^2} - \mathbb{F}_p$ 中;

当 $\ell \equiv 1 \bmod 4$ 时,

$$\Phi_\ell(1728, X) = (X - 1728)^2 \prod_{i=1}^{(\ell-1)/2} (X - a_i)^2,$$

且有 $1 + (\frac{\ell}{p})$ 个根 $a_i \in \mathbb{F}_p - \{1728\}$, 剩下的在 $\mathbb{F}_{p^2} - \mathbb{F}_p$ 中.

(2) 若 $p \equiv 2 \bmod 3$ 且 $p > 3\ell^2$, 则当 $\ell \equiv 2 \bmod 3$ 时,

$$\Phi_\ell(0, X) = \prod_{i=1}^{(\ell+1)/3} (X - a_i)^3,$$

且有 $1 + (\frac{-p}{\ell})$ 个根 $a_i \in \mathbb{F}_p^*$, 剩下的在 $\mathbb{F}_{p^2} - \mathbb{F}_p$ 中;

当 $\ell \equiv 1 \bmod 3$ 时,

$$\Phi_\ell(0, X) = X^2 \prod_{i=1}^{(\ell-1)/3} (X - a_i)^3,$$

且有 $1 + (\frac{-p}{\ell})$ 个根 $a_i \in \mathbb{F}_p^*$, 剩下的在 $\mathbb{F}_{p^2} - \mathbb{F}_p$ 中.

6.2.5　数据分析

定义 6.2　对于固定的素数 $\ell > 3$, 定义：

(i) $P_1(\ell)$ 为最大的素数 p 使得 $[E_{1728}]$ 的邻接点个数小于 $\frac{1}{2}\left(\ell - (-1)^{\frac{\ell-1}{2}}\right)$;

(ii) $P_2(\ell)$ 为最大的素数 p 使得 $[E_0]$ 的邻接边个数小于 $\frac{1}{3}(\ell - (\frac{\ell}{3}))$;

(iii) $P_1'(\ell)$ 为最大的素数 p 使得 $p \equiv 3 \bmod 4$ 且 $p < 4\ell^2$;

(iv) $P_2'(\ell)$ 为最大的素数 p 使得 $p \equiv 2 \bmod 3$ 且 $p < 3\ell^2$.

由上可知, $P_i(\ell) \leqslant P_i'(\ell)$. 而 $P_1(\ell) = P_1'(\ell)$ $(P_2(\ell) = P_2'(\ell))$ 成立时意味着我们的界 $4\ell^2$ $(3\ell^2)$ 是最好的, 此时我们称其满足 Bound I (Bound II).

我们计算了 $P_1(\ell)$, $P_2(\ell)$, 对于 $5 \leqslant \ell \leqslant 200$.

可以看出在表中, 44 在 5 到 200 之间的素数, Bound I 有 36 个素数满足. 而 47 是唯一一个 $\ell < 200$ 满足 Bound II 的, 但是 $P_2'(\ell) - P_2(\ell)$ 对于任意的 ℓ 不是很大. 所以我们得到的界是很好的.

表 6.2　当 $5 \leqslant \ell \leqslant 200$ 时 $P_1(\ell)$ 和 $P_2(\ell)$ 的数值

ℓ	5	7	11	13	17	19	23	29	31	37	41
$P_1(\ell)$	83	191	479	659	1151	1439	2111	3359	3803	5471	6719
$P_2(\ell)$	47	71	311	479	839	1031	1559	2447	2711	4079	4967
Bound	I	I	I	×	I	I	I	I	×	I	I
ℓ	43	47	53	59	61	67	71	73	79	83	89
$P_1(\ell)$	7351	8831	11171	13907	14879	17939	20147	21227	24923	27551	31667
$P_2(\ell)$	5519	6599	8231	10391	11087	13259	14951	15959	18671	20639	23687
Bound	I	I, II	I	I	I	I	I	×	×	I	I
ℓ	97	101	103	107	109	113	127	131	137	139	149
$P_1(\ell)$	37619	40787	42407	45779	47507	51071	64499	68639	75011	77279	88799
$P_2(\ell)$	28151	30491	31799	34319	35591	38231	48311	51431	56099	57839	66491
Bound	I	I	I	I	I	I	I	I	I	I	I
ℓ	151	157	163	167	173	179	181	191	193	197	199
$P_1(\ell)$	91199	98543	106187	111539	119699	128159	130927	145879	148991	155231	158363
$P_2(\ell)$	68351	73823	79631	83639	89759	95819	98207	109391	111623	116351	118751
Bound	I	×	×	I	I	I	×	×	I	I	I

6.2.6　当 $\ell = 2$ 和 3 时的情况

(1) 对于曲线 E_{1728} (此时 $p \equiv 3 \bmod 4$),

$\ell = 2$ 当 $p > 4\ell = 8$ 时, 则 $[E_{1728}]$ 有 1 条环路, 且若 I 为约化范数是 ℓ 的非主理想, 则 $[I] = [I_0]$, $[E_{1728}]$ 连接其他的顶点通过 2 条边; 当 $p = 7$ 时, 则计算模多项式 $\Phi_2(X, 1728) \equiv (X - 1728)^3 \bmod 7$, 可以得到 $[E_{1728}]$ 有 3 条环路.

$\ell = 3$ 当 $p > 4\ell = 12$ 时, 则 E_{1728} 没有环路, 且 4 条边对应 2 个理想类, $[E_{1728}]$ 通过 2 条边连接 2 个顶点; 当 $p = 7$ 时, 则计算模多项式 $\Phi_3(X, 1728) \equiv (X + 1)^4 \bmod 7$, 可以得到 E_{1728} 通过四条边连接一个顶点; 当 $p = 11$ 时, 则计算模多项式 $\Phi_3(X, 1728) \equiv (X^2 + X + 10)^2 \bmod 11$, 可以得到 E_{1728} 通过 2 条边连接 2 个顶点.

(2) 对于曲线 E_0 (此时 $p \equiv 2 \bmod 3$),

$\ell = 2$ 当 $p > 3\ell = 6$ 时, 则 E_0 没有环路, 且 I, I_0, I_{-1} 在同一个理想类中, 这说明 $[E_0]$ 通过三条边连接一个顶点; 当 $p = 5$ 时, 则计算模多项式 $\Phi_2(X, 0) \equiv X^3 \bmod 5$, 可以得到 $[E_0]$ 有 3 条环路.

$\ell = 3$ 当 $p > 3\ell = 9$ 时, 则 $[E_0]$ 有 1 条环路, 且 I, I_0, I_{-1} 在同一个理想类中, 这说明 $[E_0]$ 通过 3 条边连接一个顶点; 当 $p = 5$ 时, 则计算模多项式 $\Phi_3(X, 0) \equiv X^4 \bmod 5$, 可以得到 $[E_0]$ 有 4 条环路.

6.3　超奇异椭圆曲线同源图中 $j \in \mathbb{F}_p$ 的环路和邻接的个数

本节的结果是[24] 的主要结果. 我们将不做详细证明.

回忆在第二章最后,

(1) 当 $j \in \mathbb{F}_p$ 时，若 $\frac{1+\pi}{2} \notin \mathrm{End}(E)$，

$$\mathrm{End}(E) = \mathbb{Z} + \mathbb{Z}\frac{1+i}{2} + \mathbb{Z}\frac{j-k}{2} + \mathbb{Z}\frac{ri-k}{q}$$

其中 $(\frac{p}{q}) = -1, q \equiv 3 \bmod 8, r^2 \equiv -p \bmod q, i^2 = -q, j^2 = -p, ij = -ji = k$

(2) 当 $j \in \mathbb{F}_p$ 时，若 $\frac{1+\pi}{2} \in \mathrm{End}(E)$，

$$\mathrm{End}(E) = \mathbb{Z} + \mathbb{Z}\frac{1+j}{2} + \mathbb{Z}i + \mathbb{Z}\frac{r'i-k}{2q}$$

其中 $(\frac{p}{q}) = -1, q \equiv 3 \bmod 8, r'^2 \equiv -p \bmod 4q, i^2 = -q, j^2 = -p, ij = -ji = k$

我们知道超奇异椭圆曲线的 j 不变量在 $\mathbb{F}_p$ 时的自同态环, 那么也可以用本章前面结果同样的方式计算得到 j 不变量在 $\mathbb{F}_p$ 时回路和邻域的相关结果.

在第一章定义 δ_D 是公式 (1.1).

6.3.1　超奇异椭圆曲线同源图中 $j \in \mathbb{F}_p$ 的环路的个数

定理 6.14　[24] 对于超奇异椭圆曲线 $E, j(E) \in \mathbb{F}_p$ 时,

(1) 当 $\frac{1+\pi}{2} \notin \mathcal{O}$ 时, 若 $p > q\ell$, 顶点有 $1 + \delta_{-q}$ 条环路;

(2) 当 $\frac{1+\pi}{2} \in \mathcal{O}$ 时, 若 $p > 4q\ell$, 顶点有 $1 + \delta_{-4q}$ 条环路.

6.3.2　超奇异椭圆曲线同源图中 $j \in \mathbb{F}_p$ 的邻接的个数

定理 6.15　[24] 对于超奇异椭圆曲线 $E, j(E) \in \mathbb{F}_p$ 时,

(1) 当 $\frac{1+\pi}{2} \notin \mathcal{O}$ 时, 若 $p > q\ell^2$, 则顶点 $[E]$ 通过一重边连接到 $\ell - \delta_{-q}$ 个不同的椭圆曲线;

(2) 当 $\frac{1+\pi}{2} \in \mathcal{O}$ 时, 若 $p > 4q\ell^2$, 则顶点 $[E]$ 通过一重边连接到 $\ell - \delta_{-4q}$ 个不同的椭圆曲线.

6.3.3　超奇异椭圆曲线同源图中 $j \in \mathbb{F}_p$ 的 $\mathbb{F}_p$ 同源的个数

定理 6.16　[24] 对于超奇异椭圆曲线 $E, j(E) \in \mathbb{F}_p$ 时,

(1) 当 $\frac{1+\pi}{2} \notin \mathcal{O}$ 时, 若 $p > q\ell^2$, 则顶点 $[E]$ 有 $1 + (\frac{-p}{\ell})$ 个邻域在 $\mathbb{F}_p$ 上;

(2) $\frac{1+\pi}{2} \in \mathcal{O}$ 时, 若 $p > 4q\ell^2$, 则顶点 $[E]$ 有 $1 + (\frac{-p}{\ell})$ 个邻域在 $\mathbb{F}_p$ 上.

第 7 章　阿贝尔簇同源图的主要结果

设 n 是正整数, 令

$$\sigma(n) = \sum_{d|n,\ d\in\mathbb{N}} d.$$

记 $\sigma(n) = 0$ 若 n 不是正整数. 我们知道正整数 n 总可以写为整数的 4 平方和. 雅可比的 4 平方和定理进一步说明:

引理 7.1　(Jacobi) 丢番图方程 $x^2 + y^2 + z^2 + w^2 = n$ (n 为正整数) 的整数解的个数为

$$8\sigma(n) - 32\sigma(\frac{n}{4}) = 8\sum_{d|n,\ 4\nmid d} d.$$

特别地, 当 $n = 2$ 时, 解的个数是 24.

证明　证明可见 [64] 定理 7.3.9. □

类似地, 我们有如下结果:

引理 7.2　丢番图方程 $x^2 + xy + y^2 + z^2 + zw + w^2 = n$ 的整数解的个数为 $12\sigma(n) - 36\sigma(\frac{n}{3})$.

证明　证明可见 [65] 定理 13. □

7.1　阿贝尔簇 (ℓ,ℓ) 同源图中 $E_{1728}\times E_{1728}$ 环路的个数

回忆在第二章最后, $j = 1728$ 的超奇异椭圆曲线 E_{1728} (此时 $p \equiv 3 \bmod 4$) 的自同态环

$$\mathcal{O}_{1728} = \mathbb{Z} + \mathbb{Z}i + \mathbb{Z}\frac{1+j}{2} + \mathbb{Z}\frac{i+k}{2},$$

其中 $i^2 = -1$, $j^2 = -p$.

引理 7.3　环 $\mathcal{O}_{1728}$ 的子环 $\mathbb{Z}[i]$ 的单位群是 $\{\pm1, \pm i\}$. 在矩阵环 $M_2(\mathcal{O}_{1728})$ 中, 满足 $M^+M = I$ 的所有矩阵共 32 个, 分别为

$$\begin{pmatrix} \pm1,\pm i & 0 \\ 0 & \pm1,\pm i \end{pmatrix},\quad \begin{pmatrix} 0 & \pm1,\pm i \\ \pm1,\pm i & 0 \end{pmatrix}.$$

证明　简单计算即得. □

定理 7.4　[39] 对于 E 为 j-不变量是 1728 的超奇异椭圆曲线 E_{1728} (此时 $p \equiv 3 \bmod 4$), 当 $p > 4\ell$ 时, 在阿贝尔簇 (ℓ,ℓ) 同源图中,

(1) 当 $\ell \equiv 1 \bmod 4$ 时, $E\times E$ 有 $\ell+3$ 条环路;

(2) 当 $\ell \equiv 3 \bmod 4$ 时, $E\times E$ 有 $\ell+1$ 条环路;

(3) 当 $\ell = 2$ 时, $E \times E$ 有 3 条环路.

证明　记 $\mathcal{O} = \mathcal{O}_{1728}$. 取定 $E\times\{0\}+\{0\}\times E$ 是 $E\times E$ 的主极化除子, 它对应单位矩阵 $\boldsymbol{I}$. 计算 $E\times E$ 的环路即转化为计算 $M_2(\mathcal{O})$ 中的矩阵 $\boldsymbol{M}$ 使得 $\boldsymbol{M}^+\boldsymbol{M} = \ell\boldsymbol{I}$. 设

$$\boldsymbol{M}^+ = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \quad (a, b, c, d \in \mathcal{O}).$$

由 $\boldsymbol{M}^+\boldsymbol{M} = \ell\boldsymbol{I}$ 可知,

$$\mathrm{Nrd}(a) + \mathrm{Nrd}(b) = \ell, \quad \mathrm{Nrd}(c) + \mathrm{Nrd}(d) = \ell.$$

由于 $p > 4\ell$, 与椭圆曲线情况类似就得到

$$a, b, c, d \in \mathbb{Z}[i].$$

对矩阵 $\boldsymbol{M}$ 左数乘 $\mathbb{Z}[i]$ 的单位 $\pm 1, \pm i$ 后, 我们总可以假设

$$\boldsymbol{M}^+ = \begin{pmatrix} a & bi \\ ci & d \end{pmatrix} \quad (a, b, c, d \in \mathbb{Z}[i]). \tag{7.1}$$

由 $\boldsymbol{M}^+\boldsymbol{M} = \ell\boldsymbol{I}$ 对比系数可得:

$$\mathrm{Nrd}(a) + \mathrm{Nrd}(b) = \ell, \quad \mathrm{Nrd}(c) + \mathrm{Nrd}(d) = \ell, \quad a\bar{c} = b\bar{d}.$$

从而 $\mathrm{Nrd}(a)\,\mathrm{Nrd}(c) = \mathrm{Nrd}(b)\,\mathrm{Nrd}(d)$, 则

$$(\ell - \mathrm{Nrd}(b))(\ell - \mathrm{Nrd}(d)) = \mathrm{Nrd}(b)\,\mathrm{Nrd}(d),$$

化简即得 $\ell = \mathrm{Nrd}(b) + \mathrm{Nrd}(d)$. 进一步计算得到

$$\mathrm{Nrd}(a) = \mathrm{Nrd}(d), \quad \mathrm{Nrd}(b) = \mathrm{Nrd}(c).$$

环 $\mathbb{Z}[i]$ 是主理想整环, 故有唯一分解性质. 由于 a 和 d 的范数相同, 而 b 和 c 的范数相同, 不考虑单位 $\pm 1, \pm i$ 下, 不妨设

$$a = mAB,\ d = mA\bar{B},\ b = nCD,\ c = nC\bar{D},$$

其中 m, n 是正整数, A, B, C, D 是一些不可约因子的乘积, 且不含整数因子. 从而 $a\bar{c} = b\bar{d}$ 可写为 $mABnC\bar{C}\bar{D} = m\bar{A}BnC\bar{D}$, 即 $A\bar{C} = \bar{A}C$, 这说明 $A\bar{C} \in \mathbb{Z}$. 由于 A, C 是不可约因子乘积, 且均不被整数整除, 故 $A = C$. 此时 $A \mid a, b, c, d$, 故得

$$\mathrm{Nrd}(A) \mid \ell.$$

下面分两种情况讨论:

(1) $\mathrm{Nrd}(A) = \ell$. 此时 $a = d$, $b = c$ 且两组中有一组等于 0. 从而此时 $\ell \equiv 1 \bmod 4$, $\ell = x^2 + y^2$, M 有两种情况:

$$M = \begin{pmatrix} x + yi & 0 \\ 0 & x + yi \end{pmatrix} \quad 或 \quad M = \begin{pmatrix} x - yi & 0 \\ 0 & x - yi \end{pmatrix}.$$

(2) $\mathrm{Nrd}(A) = 1$, 此时 $a = \bar{d}$, $b = \bar{c}$. 故

$$M = \begin{pmatrix} a & bi \\ \bar{b}i & \bar{a} \end{pmatrix}.$$

不妨记 $a = a_1 + a_2 i$, $b = b_1 + b_2 i$. 由 $\mathrm{Nrd}(a) + \mathrm{Nrd}(b) = \ell$, 则有

$$a_1{}^2 + a_2{}^2 + b_1{}^2 + b_2{}^2 = \ell.$$

由引理 7.1, 此方程有 $8(\ell + 1)$ 组解. 对 M 左乘引理 7.3 出现的矩阵

$$\begin{pmatrix} \pm 1, \pm i & 0 \\ 0 & \pm 1, \pm i \end{pmatrix} \quad 或 \quad \begin{pmatrix} 0 & \pm 1, \pm i \\ \pm 1, \pm i & 0 \end{pmatrix}$$

得到的矩阵中每四个矩阵中恰好一个是(7.1) 的形式. 也就是说每 8 组解对应同一个同源, 所以同源个数 (即环路的条数) 是 $\frac{8(\ell+1)}{8} = \ell + 1$.

综合 (1) 和 (2) 即知, 当 $\ell \equiv 1 \bmod 4$ 时, 有 $\ell + 1 + 2 = \ell + 3$ 条环路; 当 $\ell \equiv 3 \bmod 4$ 时, 有 $\ell + 1$ 条环路. 当 $\ell = 2$ 时, 由计算知有三条环路, 它们对应矩阵分别是

$$\begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & i \\ i & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 + i & 0 \\ 0 & 1 + i \end{pmatrix},$$

从而 $(2, 2)$ 同源的环路有 3 条. □

7.2　阿贝尔簇 (ℓ, ℓ) 同源图中 $E_0 \times E_0$ 环路的个数

同 $j = 1728$ 的情形一样, 我们知道 $j = 0$ 的超奇异椭圆曲线 E_0 (此时 $p \equiv 2 \bmod 3$) 的自同态环

$$\mathcal{O}_0 = \mathbb{Z} + \mathbb{Z}\frac{1 + i}{2} + \mathbb{Z}\frac{i + k}{3} + \mathbb{Z}\frac{j + k}{2},$$

其中 $i^2 = -3$, $j^2 = -p$.

引理 7.5　环 $\mathcal{O}_0$ 的子环 $\mathbb{Z}[i]$ 的单位群是 $\{\pm 1, \pm\frac{1+i}{2}, \frac{1-i}{2}\}$. 在矩阵环 $M_2(\mathcal{O}_0)$ 中, 满足 $M^+ M = I$ 的所有矩阵共 72 个, 分别为

$$\begin{pmatrix} \pm 1, \pm\frac{1+i}{2}, \pm\frac{1-i}{2} & 0 \\ 0 & \pm 1, \pm\frac{1+i}{2}, \frac{1-i}{2} \end{pmatrix}, \quad \begin{pmatrix} 0 & \pm 1, \pm\frac{1+i}{2}, \pm\frac{1-i}{2} \\ \pm 1, \pm\frac{1+i}{2}, \pm\frac{1-i}{2} & 0 \end{pmatrix}.$$

定理 7.6 [39] 设 E 为 j-不变量是 0 的超奇异椭圆曲线 E_0 (此时 $p \equiv 2 \bmod 3$), 当 $p > 3\ell$ 时, 在阿贝尔簇 (ℓ, ℓ) 同源图中

(1) 若 $\ell \equiv 1 \bmod 3$, $E \times E$ 有 $\ell + 3$ 条环路;

(2) 若 $\ell \equiv 2 \bmod 3$, $E \times E$ 有 $\ell + 1$ 条环路;

(3) 若 $\ell = 3$, $E \times E$ 有 1 条环路.

证明　记 $\mathcal{O} = \mathcal{O}_0$. 取定 $E \times \{0\} + \{0\} \times E$ 是 $E \times E$ 的主极化除子, 它对应单位矩阵 $\boldsymbol{I}$. 计算 $E \times E$ 的环路即转化为计算 $M_2(\mathcal{O})$ 中的 $\boldsymbol{M}$ 使得 $\boldsymbol{M}^+\boldsymbol{M} = \ell \boldsymbol{I}$. 设

$$\boldsymbol{M}^+ = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \quad (a, b, c, d \in \mathcal{O}).$$

由 $\boldsymbol{M}^+\boldsymbol{M} = \ell \boldsymbol{I}$ 可知,

$$\mathrm{Nrd}(a) + \mathrm{Nrd}(b) = \ell, \qquad \mathrm{Nrd}(c) + \mathrm{Nrd}(d) = \ell.$$

由于 $p > 3\ell$, 与椭圆曲线情况同样论述即得

$$a, b, c, d \in \mathbb{Z}[\frac{1+i}{2}].$$

对矩阵 $\boldsymbol{M}$ 左数乘 $\mathbb{Z}[i]$ 的单位 $\pm\frac{1+i}{2}, \frac{1-i}{2}$ 后, 我们总可以假设

$$\boldsymbol{M}^+ = \begin{pmatrix} a & b\frac{1+i}{2} \\ c\frac{-1+i}{2} & d \end{pmatrix} \quad (a, b, c, d \in \mathbb{Z}[\frac{1+i}{2}]). \tag{7.2}$$

由 $\boldsymbol{M}^+\boldsymbol{M} = \ell \boldsymbol{I}$ 对比系数可得:

$$\mathrm{Nrd}(a) + \mathrm{Nrd}(b) = \ell, \qquad \mathrm{Nrd}(c) + \mathrm{Nrd}(d) = \ell, \qquad a\bar{c} = b\bar{d}.$$

从而 $\mathrm{Nrd}(a)\,\mathrm{Nrd}(c) = \mathrm{Nrd}(b)\,\mathrm{Nrd}(d)$, 则

$$(\ell - \mathrm{Nrd}(b))(\ell - \mathrm{Nrd}(d)) = \mathrm{Nrd}(b)\,\mathrm{Nrd}(d),$$

化简即得 $\ell = \mathrm{Nrd}(b) + \mathrm{Nrd}(d)$. 进一步计算得到

$$\mathrm{Nrd}(a) = \mathrm{Nrd}(d), \qquad \mathrm{Nrd}(b) = \mathrm{Nrd}(c).$$

环 $\mathbb{Z}[\frac{1+i}{2}]$ 是主理想整环, 故有唯一分解性质. 由于 a, d 的范数相同, 而 b, c 的范数相同, 不考虑单位 $\pm 1, \pm\frac{1+i}{2}, \pm\frac{1-i}{2}$ 下, 不妨设

$$a = m\boldsymbol{A}\boldsymbol{B}, d = m\boldsymbol{A}\bar{\boldsymbol{B}}, b = n\boldsymbol{C}\boldsymbol{D}, c = n\boldsymbol{C}\bar{\boldsymbol{D}},$$

其中 m,n 为正整数, $\boldsymbol{A},\boldsymbol{B},\boldsymbol{C},\boldsymbol{D}$ 为一些不可约因子的乘积, 且不含整数因子. 从而 $a\bar{c}=b\bar{d}$ 可写为 $m\boldsymbol{A}\boldsymbol{B}n\bar{\boldsymbol{C}}\bar{\boldsymbol{D}}=m\bar{\boldsymbol{A}}\boldsymbol{B}n\boldsymbol{C}\bar{\boldsymbol{D}}$, 即 $\boldsymbol{A}\bar{\boldsymbol{C}}=\bar{\boldsymbol{A}}\boldsymbol{C}$, 这说明 $\boldsymbol{A}\bar{\boldsymbol{C}}\in\mathbb{Z}$. 由于 $\boldsymbol{A},\boldsymbol{C}$ 为不可约因子乘积, 且均不被整数整除, 则 $\boldsymbol{A}=\boldsymbol{C}$. 此时 $\boldsymbol{A}\mid a,b,c,d$, 故得

$$\mathrm{Nrd}(\boldsymbol{A})\mid\ell.$$

下面分两种情况讨论:

(1) $\mathrm{Nrd}(\boldsymbol{A})=\ell$, 此时 $a=d$, $b=c$ 且两组中有一组等于 0. 从而此时 $\ell\equiv 1 \bmod 3$, $\ell=(x+\frac{y}{2})^2+(\frac{y}{2})^2$, $\boldsymbol{M}$ 有两种情况:

$$\boldsymbol{M}=\begin{pmatrix} x+y\frac{1+i}{2} & 0\\ 0 & x+y\frac{1+i}{2}\end{pmatrix}\quad 或\qquad \boldsymbol{M}=\begin{pmatrix} x+y\frac{1-i}{2} & 0\\ 0 & x+y\frac{1-i}{2}\end{pmatrix}.$$

(2) $\mathrm{Nrd}(\boldsymbol{A})=1$, 此时 $a=\bar{d}$, $b=\bar{c}$. 故

$$\boldsymbol{M}=\begin{pmatrix} a & b\frac{1+i}{2}\\ \bar{b}\frac{-1+i}{2} & \bar{a}\end{pmatrix}.$$

不妨记 $a=a_1+a_2\frac{1+i}{2}$, $b=b_1+b_2\frac{1+i}{2}$. 由 $\mathrm{Nrd}(a)+\mathrm{Nrd}(b)=\ell$, 则有

$${a_1}^2+a_1a_2+{a_2}^2+{b_1}^2+b_1b_2+{b_2}^2=\ell.$$

由引理 7.2, 此方程有 $12(\ell+1)$ 组解. 对 $\boldsymbol{M}$ 左乘引理 7.5 出现的矩阵

$$\begin{pmatrix} \pm1,\pm\frac{1+i}{2},\pm\frac{1-i}{2} & 0\\ 0 & \pm1,\pm\frac{1+i}{2},\frac{1-i}{2}\end{pmatrix},\quad \begin{pmatrix} 0 & \pm1,\pm\frac{1+i}{2},\pm\frac{1-i}{2}\\ \pm1,\pm\frac{1+i}{2},\pm\frac{1-i}{2} & 0\end{pmatrix}$$

得到的矩阵中每六个矩阵中恰好一个是(7.2) 的形式. 也就是说每 12 组解对应同一个同源, 所以同源个数 (即环路的条数) 是 $\frac{12(\ell+1)}{12}=\ell+1$.

综合 (1) 和 (2) 即知, 当 $\ell\equiv 1 \bmod 3$ 时, 有 $\ell+1+2=\ell+3$ 条环路; 当 $\ell\equiv 2 \bmod 3$ 时, 有 $\ell+1$ 条环路. 当 $\ell=3$ 时, 由计算知有一条环路, 它对应的矩阵是:

$$\begin{pmatrix} i & 0\\ 0 & i\end{pmatrix}.$$

从而 $(3,3)$ 同源的环路有一条. □

第 8 章　总结与展望

8.1　椭圆曲线同源图研究总结与展望

我们通过给出定义在 $\mathbb{F}_p$ 上的超奇异椭圆曲线的自同态环, 求解丢番图方程, 来得到：

(1) j 在 $\mathcal{G}_\ell(\overline{\mathbb{F}_p})$ 中环路的个数;

(2) j 在 $\mathcal{G}_\ell(\overline{\mathbb{F}_p})$ 中邻接的个数;

(3) j 与每个邻接之间边的重数;

(4) 从 j 出发的 $\mathbb{F}_p$ 同源的个数.

我们给出了 j 是 0 和 1728 的具体结果, 但是对于定义在 $\mathbb{F}_p$ 上的超奇异椭圆曲线, 自同态环的参数中有 q, 这直接影响到给出的界里面含有 q, 这看起来并不是最好的结果, 我们希望 $q < cp^{1-\epsilon}$, 这样关于界就可以只有 p 和 ℓ 之间的关系. 另一方面, 关于定义在 $\mathbb{F}_{p^2}\backslash\mathbb{F}_p$ 上的超奇异椭圆曲线的自同态环我们还不清楚, 这影响到我们给出所有 $\mathbb{F}_{p^2}$ 上的超奇异椭圆曲线的结果.

8.2　(ℓ,ℓ) 同源图展望

我们通过给出 $E_{1728}\times E_{1728}$ 和 $E_0\times E_0$ 的自同态环和矩阵的对应关系, 求解丢番图方程, 来得到其在 (ℓ,ℓ) 同源图中的环路的个数.

但是对于邻域的计算由于在阿贝尔簇中没有和椭圆曲线一样的 Deuring 对应定理, 我们需要发现新的方法去计算邻域的个数.

对于其他的顶点, 尤其是超椭圆曲线的雅可比簇 Jac(C) 我们仍需要新的工具去计算, 比如其对应的矩阵, 这就和椭圆曲线中计算 $\mathbb{F}_{p^2}\backslash\mathbb{F}_p$ 的点的自同态环一样是不容易的, 所以可能需要更多的工具.

8.3　密码学的应用展望

椭圆曲线密码依旧是热门的密码学问题, 其上主要的数学问题就是同源图的计算和同源的计算, 对于同源图的计算我们得到了 $\mathbb{F}_p$ 上的一部分结果, 但是这对于攻击还是不够的, 需要进一步的对所有超奇异椭圆曲线得到类似的结果. 另一方面, 对于计算同源的问题仍需要更多的关注, 这也是攻击 SIDH 的关键. 当然这两个问题都和自同态环有着紧密的联系.

对于后来兴起的阿贝尔簇上的同源密码, 是近两年比较热的, 其在椭圆曲线上做了进一步的推广, 同样的其同源图的计算和同源的计算也是需要解决的关键

问题. 但是这些数学问题相较于椭圆曲线而言会更难需要更多的代数几何等知识, 工具也更多.

参 考 文 献

[1] MILLER V. Use of elliptic curves in cryptography [J]. Advances in cryptology-crypto, 1986, 85: 417-426.

[2] KOBLITZ N. Elliptic curve cryptosystems [J]. Math. Comp., 1987.

[3] GALBRAITH S D, GAUDRY P. Recent progress on the elliptic curve discrete logarithm problem [J]. Designs Codes Cryptography, 2016, 78(1): 51-72.

[4] SHOR P. Algorithms for quantum computation: discrete logarithms and factoring [J]. In Proceedings of 35th Annual Symposium on the Foundations of Computer Science, IEEE Computer Society Press, Los Alamitos, CA, 1994: 124-134.

[5] CHARLES D X, LAUTER K E, GOREN E Z. Cryptographic hash functions from expander graphs [J]. Journal of Cryptology, 2008, 22(1): 93-113.

[6] STOLBUNOV A. Constructing public-key cryptographic schemes based on class group action on a set of isogenous elliptic curves [J]. Advances in Mathematics of Communications, 2010, 4(2): 215-235.

[7] FEO L D, JAO D, PLUT J. Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies [J]. Journal of Mathematical Cryptology, 2014, 8: 209-247.

[8] CASTRYCK W, LANGE T, MARTINDALE C, et al. Csidh: an efficient post-quantum commutative group action [C]//International Conference on the Theory and Application of Cryptology and Information Security. Springer, 2018: 395-427.

[9] CHILDS A, JAO D, SOUKHAREV V. Constructing elliptic curve isogenies in quantum subexponential time [J]. Journal of Mathematical Cryptology, 2014, 8(1): 1-29.

[10] BIASSE J, JAO D, SANKAR A. A quantum algorithm for computing isogenies between supersingular elliptic curves [C]//International Conference on Cryptology in India. Springer, 2014: 428-442.

[11] DELFS C, GALBRAITH S D. Computing isogenies between supersingular elliptic curves over f-p [J]. Designs Codes Crytography, 2016.

[12] LOVE J, BONEH D. Supersingular curves with small noninteger endomorphisms [J]. Open Book Series, 2020, 4(1): 7-22.

[13] KOHEL D, LAUTER K, PETIT C, et al. On the quaternion ℓ-isogeny path problem [J]. LMS Journal of Computation and Mathematics, 2014, 17(A): 418-432.

[14] CASTRYC W, PANNY L, VERCAUTEREN F. Rational isogenies from irrational endomorphisms [C]//EUROCRYPT 2020: volume 12106. 2020: 523-548.

[15] KOHEL D. Endomorphism rings of elliptic curves over finite fields [D]. University of Cali-

fornia, Berkeley, 1996.

[16] CERVINO J. Supersingular elliptic curves and maximal quaternionic orders [J]. 2004.

[17] BISSON G, SUTHERLAND A. Computing the endomorphism ring of an ordinary elliptic curve over a finite field [J]. Journal of Number Theory, 2011, 131(5): 815-831.

[18] CHEVYREV I, GALBRAITH S. Constructing supersingular elliptic curves with a given endomorphism ring [J]. LMS Journal of Computation and Mathematics, 2014, 17(A): 71-91.

[19] BANK E, CAMACHO-NAVARRO C, EISENTRAGER K, et al. Cycles in the supersingular ℓ-isogeny graph and corresponding endomorphisms [M]//Research Directions in Number Theory. Springer, 2019: 41-66.

[20] EISENTRäGER K, HALLGREN S, LEONARDI C, et al. Computing endomorphism rings of supersingular elliptic curves and connections to path-finding in isogeny graphs [J]. Open Book Series, 2020, 4(1): 215-232.

[21] ADJ G, AHMADI O, MENEZES A. On isogeny graphs of supersingular elliptic curves over finite fields [J]. Finite Fields and Their Applications, 2019, 55(JAN.): 268-283.

[22] OUYANG Y, XU Z. Loops of isogeny graphs of supersingular elliptic curves at $j = 0$ [J]. Finite Fields And Their Applications, 2019, 58: 174-176.

[23] LI S, OUYANG Y, XU Z. Neighborhood of the supersingular elliptic curve isogeny graph at $j = 0$ and 1728 [J]. 2020, 61(101600).

[24] LI S, OUYANG Y, XU Z. Endomorphism rings of supersingular elliptic curves over $\mathbb{F}_p$ [J]. Finite Fields and Their Applications, 2020, 62: 101619.

[25] EISENTRAGER K, HALLGREN S, LAUTER K, et al. Supersingular isogeny graphs and endomorphism rings: reductions and solutions [C]//Annual International Conference on the Theory and Applications of Cryptographic Techniques. Springer, 2018: 329-368.

[26] ONUKI H, AIKAWA Y, TAKAGI T. The existence of cycles in the supersingular isogeny graphs used in sike. [J]. IACR Cryptol. ePrint Arch., 2020, 2020: 439.

[27] MCMURDY K. Explicit representation of the endomorphism rings of supersingular elliptic curves [Z]. 2014.

[28] IBUKIYAMA T. On maximal orders of division quaternion algebras over the rational number field with certain optimal embeddings [J]. Nagoya Mathematical Journal, 1982, 88: 181-195.

[29] IONICA S, THOME E. Isogeny graphs with maximal real multiplication [J]. Journal of Number Theory, 2020, 207: 385-422.

[30] SPRINGER C. Computing the endomorphism ring of an ordinary abelian surface over a finite field [J]. Journal of Number Theory, 2019, 202: 430-457.

[31] FLYNN E V, YAN B T. Genus two isogeny cryptography [M]. International Conference on Post-quantum Cryptography, 2019.

[32] CASTRYCK W, DECRU T, SMITH B. Hash functions from superspecial genus-2 curves using richelot isogenies [J]. Journal of Mathematical Cryptology, 2020, 14(1): 268-292.

[33] KATSURA T, TAKASHIMA K. Counting richelot isogenies between superspecial abelian surfaces [J]. 2020.

[34] JORDAN B W. Isogeny graphs of superspecial abelian varieties [J]. 2021.

[35] COSTELLO C, SMITH B. The supersingular isogeny problem in genus 2 and beyond [C]// International Conference on Post-Quantum Cryptography. Springer, 2020: 151-168.

[36] FLORIT E, SMITH B. Automorphisms and isogeny graphs of abelian varieties, with applications to the superspecial richelot isogeny graph [J]. 2021.

[37] FLORIT E, SMITH B. An atlas of the richelot isogeny graph [J]. 2021.

[38] KATSURA T. On decomposed richelot isogenies of curves of genus 3 [J]. arXiv preprint arXiv:2103.01800, 2021.

[39] OUYANG Y, XU Z. Loops of isogeny graphs of superspecial abelian varieties at $e_{1728} \times e_{1728}$ and $e_0 \times e_0$ [J]. 2021.

[40] SILVERMAN J H. The arithmetic of elliptic curves: volume 106 [M]. Springer Science, 2009.

[41] SILVERMAN J H. Advanced topics in the arithmetic of elliptic curves: volume 151 [M]. Springer Science, 1994.

[42] SUTHERLAND A. Elliptic curves [M]. https://math.mit.edu/classes/18.783/2019/lectures.html.

[43] COX D A. Primes of the form x^2+ny^2: Fermat, class field theory, and complex multiplication: volume 34 [M]. John Wiley & Sons, 2011.

[44] TATE J. Endomorphisms of abelian varieties over finite fields [J]. Inventiones mathematicae, 1966, 2(2): 134-144.

[45] SCHOOF R. Nonsingular plane cubic curves over finite fields [J]. Journal of combinatorial theory, Series A, 1987, 46(2): 183-211.

[46] WATERHOUSE W. Abelian varieties over finite fields [C]//Annales scientifiques de lEcole normale superieure: volume 2. 1969: 521-560.

[47] VOIGHT J. Quaternion algebras: volume 288 [M]. Springer Science, 2021.

[48] MCMURDY K, LAUTER K. Explicit generators for endomorphism rings of supersingular elliptic curves [M]. Citeseer, 2004.

[49] HARTSHORNE R. Algebraic geometry: volume 52 [M]. Springer Science, 2013.

[50] HINDRY M, SILVERMAN J H. Diophantine geometry: an introduction: volume 201 [M]. Springer Science & Business Media, 2013.

[51] IGUSA J I. Arithmetic variety of moduli for genus two [J]. Annals of Mathematics, 1960: 612-649.

[52] GALBRAITH S D. Mathematics of public key cryptography [M]. Cambridge University

Press, 2012.

[53] MILNE J S. Abelian varieties [J]. Arithmetic geometry, 1986: 103-150.

[54] VAN DER GEER G, MOONEN B. Abelian varieties [J]. Book in preparation, 2007: 71.

[55] MUMFORD D, RAMANUJAM C P, MANIN I I. Abelian varieties: volume 2 [M]. Oxford university press Oxford, 1974.

[56] OORT F. Which abelian surfaces are products of elliptic curves? [J]. Mathematische Annalen, 1975, 214(1): 35-47.

[57] LI K Z, OORT F. Moduli of supersingular abelian varieties: volume 1680 [M]. Springer Science, 1998.

[58] PEREGO A. Introduction to algebraic surfaces [J]. 2009.

[59] SMITH B. Explicit endomorphisms and correspondences [J]. 2005.

[60] IBUKIYAMA T, KATSURA T, OORT F. Supersingular curves of genus two and class numbers [J]. Compositio Mathematica, 1986, 57(2): 127-152.

[61] COSTACHE A, FEIGON B, LAUTER K, et al. Ramanujan graphs in cryptography [M]// Research Directions in Number Theory. Springer, 2019: 1-40.

[62] GRAU J, MIGUEL C, OLLER-MARCEN A M. On the structure of quaternion rings over $\mathbb{Z}/n\mathbb{Z}$ [J]. Advances in Applied Clifford Algebras, 2015, 25(4): 875-887.

[63] ALPERIN J, BELL R. Group and representation: volume 162 [M]. Springer Science, 1995.

[64] 李文威. 模形式初步 [M]. 科学出版社, 2020.

[65] HUARD J G, OU M, SPEARMAN B K, et al. Elementary evaluation of certain convolution sums involving divisor functions [J]. Number theory for the Millennium, 2002, 2: 229-274.

致　谢

时光荏苒, 岁月如梭, 在中国科学技术大学五年的硕博连读研究生生涯即将划上句号. 回想起在科大的点点滴滴, 一切都历历在目, 宛如昨日. 这里有陪伴我成长的导师和同学, 也有我从稚嫩走向成熟的一步步成长. 在毕业之际, 我想对我的老师, 同学和家人们表达深深的感谢.

首先, 我要特别感谢我的导师欧阳毅教授. 欧阳老师渊博的学识, 严谨的治学态度和平易近人的为人处事风格深深影响着我. 老师总是循循善诱, 不厌其烦地指导我. 我的所有论文都是在欧阳老师的指导下完成的, 并且本文在选题, 撰写, 修改以及最终定稿都得到了欧阳老师的悉心指导. 欧阳老师宽厚待人, 和蔼可亲的性格态度, 严谨务实, 孜孜不倦的学术作风, 让我如沐春风, 是我一生都要追求和学习的目标和楷模. 在此, 我向欧阳老师表达我最诚挚的谢意.

感谢信息技术学院的胡红钢教授. 胡老师让我们参加他的组会, 积极学习密码学知识, 提出的建议让我受益无穷. 胡老师广阔的学识和认真的工作态度也是我学习的对象.

感谢李宋宋师姐在学习上对我的支持, 帮助和鼓励. 很开心可以和她一起讨论问题, 合作完成两篇文章. 感谢许跃师兄和李加宁师兄帮我解答很多学习上的问题. 感谢我的师弟谢贤红, 王森等对我的帮助, 帮我分担很多压力. 感谢胡老师的学生王辈师姐, 张霄涵, 戴立等对我的帮助. 也感谢马文秀, 邱意雅和苏鑫陪我度过的快乐时光. 也感谢我的朋友张冠凯, 原宏敏, 欧阳艳敏, 王钊等对我的照顾. 感谢我的舍友叶春阳和朱永拼这么多年的关照. 感谢中国科学技术大学数学系的各位老师, 你们不仅交给了我知识, 也为我创造了良好的学习环境, 使我能够安心的做科研.

最后, 我下感谢我的父母, 要是没有你们的支持我可能也不会一路走到现在, 让我可以完成学业, 做出更好的成就回报祖国和社会, 并实现自己的理想.

在读期间发表的学术论文与取得的研究成果

已发表论文

1. Yi Ouyang, Zheng Xu. Loops of isogeny graphs of supersingular elliptic curves at $j = 0$[J], Finite Fields and Their Applications,Volume 58, 2019, 174-176.
2. Songsong Li, Yi Ouyang, Zheng Xu. Neighborhood of the supersingular elliptic curve isogeny graph at $j = 0$ and 1728[J], Finite Fields and Their Applications,Volume 61, 2020, 101600.
3. Songsong Li, Yi Ouyang, Zheng Xu. Endomorphism rings of supersingular elliptic curves over $\mathbb{F}_p$[J], Finite Fields and Their Applications,Volume 62, 2020, 101619.

待发表论文

1. Yi Ouyang, Zheng Xu. Loops of isogeny graphs of superspecial abelian varieties at $E_{1728} \times E_{1728}$ and $E_0 \times E_0$, preprint.