中国科学: 数学 2021 年 第 51 卷 第 10 期: 1635 ~ 1654
SCIENTIA SINICA Mathematica
论 文

Abel p- 分歧扭子群和新 Cohen-Lenstra 猜想

献给冯克勤教授 80 华诞

李加宁, 欧阳毅*, 许跃

中国科学技术大学数学科学学院, 合肥 230026

E-mail: lijn@ustc.edu.cn, yiouyang@ustc.edu.cn, wasx250@mail.ustc.edu.cn

收稿日期: 2020-09-30; 接受日期: 2021-04-01; 网络出版日期: 2021-09-28; * 通信作者
安徽省量子信息先导 (批准号: AHY150200) 和中央高校基础科学研究基金 (批准号: WK0010000058) 资助项目

摘要 本文首先回顾数域 K 的 Abel p- 分歧理论特别是其 $\mathcal{T}_p$- 群, 并给出一般 Cohen-Lenstra 猜想的架构. 对于全体实 (虚) 二次域及其几类子族, 本文提出 $\mathcal{T}_p(K)$ 的分布满足新的 Cohen-Lenstra 猜想. 后者解释了 Shanks 等 (1999) 对于 2- 进 L 函数特殊值的分布猜测, 并给出基本单位迹的分布猜想. 本文给出理论结果和计算数据来支持这些猜想.

关键词 Cohen-Lenstra 猜想 二次域 Abel p- 分歧群 类群 基本单位

MSC (2020) 主题分类 11R45, 11R11, 11R37

1 引言

设 p 是素数. 对于数域 K, 令 $M = M(K,p)$ 是 K 的极大 p- 分歧 Abel 射影 -p 扩张. 由类域论可知 $\mathrm{Gal}(M/K)$ 是有限生成 $\mathbb{Z}_p$- 模, 它的秩是 $r_2(K)+\delta_p(K)+1$, 其中 $r_2(K)$ 是 K 的复素位的个数而 $\delta_p(K)\geqslant 0$ 是 K 在 p 处的 Leopoldt 缺陷. Leopoldt 猜想即为 $\delta_p(K)=0$ 对于所有 p 和 K 成立, 它在 $K/\mathbb{Q}$ 是 Abel 扩张情形时已经得到证明. 我们称 $\mathrm{Gal}(M/K)$ 的 $\mathbb{Z}_p$- 扭子群为 K 的 $\mathcal{T}_p$- 群, 记为 $\mathcal{T}_p(K)$. 这是一个有限 Abel p 群. 对于 $\mathrm{Gal}(M/K)$ 和 $\mathcal{T}_p(K)$ 的研究, 即所谓的 Abel p- 分歧理论, 吸引了很多研究者的注意 (参见文献 [1,2]).

在此前的研究中 (如文献 [3]), 人们着重研究 p- 有理情形, 即 $\mathcal{T}_p$- 群平凡情形. 特别地, Pitoun 和 Varescon [4] 发展了一套算法计算 $\mathcal{T}_p$- 群并研究 p- 有理二次域的比例. 他们发现所获得的数据与 Cohen-Lenstra 猜想很吻合: 对于 $5\leqslant p\leqslant 47$, 在所有二次域 $\mathbb{Q}(\sqrt{d})$ (其中 d 无平方因子且 $0<d\leqslant 10^9$) 中, $\mathcal{T}_p$- 群平凡的二次域的比值大约是 $\prod_{i=1}^{\infty}(1-p^{-i})$. 在文献 [4] 中, 作者还言及考虑了 $\mathcal{T}_p$- 群的群结构分布, 但我们并没有在该文献中或者之后文献中发现他们在这方面的任何继续研究.

本文对于所有实或者是虚的二次域的 $\mathcal{T}_p$- 群, 提出 Cohen-Lenstra 猜想 (见猜想 4.1). 具体地, 我们猜想对于 $p\geqslant 5$, 实二次域 (或者虚二次域) 的 $\mathcal{T}_p$- 群对于权重函数 ω_0 (或者 ω_1) 是均匀分布的.

英文引用格式: Li J N, Ouyang Y, Xu Y. Abelian p-ramification groups and new Cohen-Lenstra heuristics (in Chinese). Sci Sin Math, 2021, 51: 1635–1654, doi: 10.1360/SSM-2020-0294

Pitoun 和 Varescon 的观测结果是我们猜想的一个特殊情形. 对于坏的素数 $p=2,3$, 我们需要将 $\mathcal{T}_p$ 用 $p\mathcal{T}_p$ 代替, 如同类群情形的局部 Cohen-Lenstra 猜想. 更进一步地, 在坏素数 $p=2$ 的情形, 我们给出了虚二次域的 $\mathcal{T}_2$- 群的 4- 秩密度分布公式, 这对于我们的猜想是极大佐证.

在 Shanks 等 [5] 工作的启发下, 对于一些特殊的实或者虚二次域子族, 我们给出扩展的 Cohen-Lenstra 猜想. 下面描述 Shanks 等在这方面的工作.

对于无平方因子的正整数 m, 令 χ_m 是 $\mathbb{Q}(\sqrt{m})$ 对应的 Dirichlet 特征, $L_2(s,\chi_m)$ 是对应的 2- 进 L- 函数. 在文献 [5] 中, 在 $\mathbb{Q}(\sqrt{-m})$ 的分圆 $\mathbb{Z}_2$- 扩张的岩泽 λ 常数等于 1 的情形, Shanks 等研究了特殊值 $L_2(0,\chi_m)$ 和 $L_2(1,\chi_m)$ 的 2- 进表现. 他们给出如下猜想 (参见文献 [5, 第 1253 页]):

猜想 1.1 对于整数 $k\geqslant 0$,

$$\lim_{X\to\infty}\frac{\#\{l\text{ 为素数}: l\leqslant X,\ l\equiv 9\ (\mathrm{mod}\ 16)\text{ 且 }\nu_2(L_2(0,\chi_l))=k+2\}}{\#\{l\text{ 为素数}: l\leqslant X\text{ 且 }l\equiv 9\ (\mathrm{mod}\ 16)\}}=\frac{1}{2^{k+1}},\tag{1.1}$$

$$\lim_{X\to\infty}\frac{\#\{l\text{为素数}: l\leqslant X, l\equiv 9\ (\mathrm{mod}\ 16)\text{ 且 }\nu_2(L_2(1,\chi_l))=k+2\}}{\#\{l\text{ 为素数}: l\leqslant X\text{ 且 }l\equiv 9\ (\mathrm{mod}\ 16)\}}=\frac{1}{2^{k+1}},\tag{1.2}$$

这里 ν_2 是正则加性 2- 进赋值, 即 $\nu_2(2)=1$.

对于其他的一些实二次域子族, 如 $\{\mathbb{Q}(\sqrt{2l})\}_{l\equiv 9\ (\mathrm{mod}\ 16)}$、$\{\mathbb{Q}(\sqrt{6l})\}_{l\equiv 3\ (\mathrm{mod}\ 8)}$ 和 $\{\mathbb{Q}(\sqrt{5l})\}_{l\equiv 5\ (\mathrm{mod}\ 8)}$ 等, 他们也发现类似的现象. 我们将证明这个猜想在 $k=0$ 和 $k=1$ 情形是正确的.

等式 (1.1) 可以用类群的语言来描述. 设 $h(-m)$ 是 $\mathbb{Q}(\sqrt{-m})$ 的类数, χ_{-4} 是模 4 的非平凡 Dirichlet 特征. 若 $\mathbb{Q}(\sqrt{-m})$ 既非 $\mathbb{Q}(\sqrt{-1})$ 也非 $\mathbb{Q}(\sqrt{-3})$, 则

$$L_2(0,\chi_m)=(1-\chi_m\chi_{-4}(2))h(-m).$$

因此 (1.1) 即是说, 在同余类 9 (mod 16) 的素数中, 满足 $\mathbb{Q}(\sqrt{-l})$ 的 2- 类群同构于 $\mathbb{Z}/2^{k+2}\mathbb{Z}$ 的素数 l 的密度是 $1/\#\mathrm{Aut}(\mathbb{Z}/2^{k+2}\mathbb{Z})=1/2^{k+1}$. 正如文献 [5, 第 1253 页] 所指出, 这可以认为是关于类群的一个扩展的 Cohen-Lenstra 猜想.

我们说明 (1.2) 可以认为是关于 $\mathcal{T}_2$- 群的扩展 Cohen-Lenstra 猜想. 简记 $\mathcal{T}_p(\mathbb{Q}(\sqrt{m}))$ 为 $\mathcal{T}_p(m)$. Coates [6] 证明了联系 $|\mathcal{T}_p(m)|$ 与 $L_p(1,\chi_m)$ 的下述公式:

$$|\mathcal{T}_p(m)|=(p\text{- 进单位})\cdot\frac{p^2[\mathbb{Q}(\sqrt{m})\cap\mathbb{Q}^{p,\mathrm{cyc}}:\mathbb{Q}]\cdot L_p(1,\chi_m)}{2(p-\chi_m(p))\cdot\prod_{\mathfrak{p}\mid p}N\mathfrak{p}},\tag{1.3}$$

这里 $\mathbb{Q}^{p,\mathrm{cyc}}$ 是 $\mathbb{Q}$ 的分圆 $\mathbb{Z}_p$- 扩张, 乘积过 $\mathbb{Q}(\sqrt{m})$ 中所有位于 p 上的素理想, N 是 $\mathbb{Q}(\sqrt{m})$ 到 $\mathbb{Q}$ 的范映射. 对于素数 $l\equiv 9\ (\mathrm{mod}\ 16)$, 不难证明 $\mathcal{T}_2(l)$ 是循环群 (参见命题 2.2). 那么 (1.2) 可以重新解释为: 对于 $k\geqslant 0$, 总有

$$\lim_{X\to\infty}\frac{\#\{l\text{ 为素数}: l\leqslant X,\ l\equiv 9\ (\mathrm{mod}\ 16)\text{ 且 }\mathcal{T}_2(l)\cong\mathbb{Z}/2^{k+1}\mathbb{Z}\}}{\#\{l\text{ 为素数}: l\leqslant X,\ l\equiv 9\ (\mathrm{mod}\ 16)\}}=\frac{1}{2^{k+1}}.\tag{1.4}$$

我们的新解释的优点是, (1.2) 不能直接推广到奇二次特征情形, 因为此时的 p- 进 L- 函数恒为 0, 但 $\mathcal{T}_p$- 群对于所有虚二次域均有定义. 第 4 节将对二次域一些子族的 $\mathcal{T}_2$- 群提出扩展 Cohen-Lenstra 猜想 (猜想 4.2), (1.4) 是它的特殊情形.

这里给出猜想 4.2 另一个有趣推论. 设 l 是素数, $a_l+b_l\sqrt{l}$ 是 $\mathbb{Q}(\sqrt{l})$ 的基本单位. 对于 $l\equiv 1,3,7\ (\mathrm{mod}\ 8)$, 熟知 $a_l\in 2\mathbb{Z}$ 且 $b_l\in\mathbb{Z}$. 更进一步地, 若 $l\equiv 3\ (\mathrm{mod}\ 8)$, 则 $\nu_2(a_l)=1$; 若 $l\equiv 7\ (\mathrm{mod}\ 16)$, 则 $\nu_2(a_l)=3$ (参见文献 [5]). 但对于 $i\geqslant 4$, 并不存在同余条件来刻画素数 l 使得 $\nu_2(a_l)=i$. 基于 Coates 的公式, 猜想 4.2 给出如下关于基本单位的猜想:

猜想 1.2 对于每个非负整数 k, 下列式子均成立:

$$\lim_{X\to\infty}\frac{\#\{l\text{ 为素数}: l\leqslant X,\ l\equiv 1\ (\mathrm{mod}\ 8),\ \nu_2(a_l)=k+2\}}{\#\{l\text{ 为素数}:\ l\leqslant X,\ l\equiv 1\ (\mathrm{mod}\ 8)\}}=\frac{1}{2^{k+1}},\tag{1.5}$$

$$\lim_{X\to\infty}\frac{\#\{l\text{ 为素数}: l\leqslant X,\ l\equiv -1\ (\mathrm{mod}\ 8),\ \nu_2(a_l)=k+3\}}{\#\{l\text{ 为素数}:\ l\leqslant X,\ l\equiv -1\ (\mathrm{mod}\ 8)\}}=\frac{1}{2^{k+1}}.\tag{1.6}$$

本文余下内容组织如下. 第 2 节回顾 $\mathcal{T}_p$- 群的基本性质. 第 3 节给出局部 Cohen-Lenstra 猜想的基本知识, 给出类群情形时局部猜想的描述, 并提出几类二次域子族的 2- 类群的扩展 Cohen-Lenstra 猜想. 第 4 节给出 $\mathcal{T}_p$- 群的 Cohen-Lenstra 猜想并证明一些密度结果来支持我们的猜想. 最后一节给出猜想的数值依据.

本文将使用如下记号:

(1) p 和 l 都是素数, $\mathbb{Z}_p$ 是 p- 进整数环, μ_p 是 p- 次单位根群.

(2) 对于无平方因子整数 m, $\mathrm{Cl}(m)$、$\mathrm{Cl}_p(m)$、$h(m)$、$\mathcal{T}_p(m)$ 和 $t_p(m)$ 分别是二次域 $\mathbb{Q}(\sqrt{m})$ 的类群、p- 类群、类数、$\mathcal{T}_p$- 群和 $\mathcal{T}_p$- 群的阶.

(3) A 是离散赋值环, π 是它的一个素元, $k=A/\pi A$ 是剩余类域且总假设它是有限域. $\mathcal{M}_A$ 是有限 A- 模自同构类集合. 对于有限 A- 模 G, $\mathrm{rk}_kG:=\dim_k G/\pi G$, $\mathrm{Aut}_A(G)$ 是 G 的 A- 自同构群.

(4) 对于 $A=\mathbb{Z}_p$, 有限 Abel p- 群 H 的 p- 秩定义为 $\mathrm{rk}_pH:=\dim_{\mathbb{F}_p}H/pH$, 集合 $V_j:=\{\mathbb{Z}/2^k\mathbb{Z}: k\geqslant j\}\subseteq\mathcal{M}_{\mathbb{Z}_2}$.

2 数域的 $\mathcal{T}_p$- 群

2.1 $\mathcal{T}_p$- 群的研究工作概述

回顾数域 $\mathcal{T}_p$- 群的相关结果, 这里主要是 Coates[6] 和 Gras[1,7,8] 等的工作. 对于它的研究是 Abel p- 分歧理论的一部分, 详情参见文献 [1,7].

设 K 是数域. 令 $M=M(K,p)$ 是 K 的极大 p- 分歧 Abel 射影 -p 扩张. 由类域论知, $\mathrm{Gal}(M/K)$ 是有限生成 $\mathbb{Z}_p$- 模, 其秩为 $r_2(K)+\delta_p(K)+1$, 其中 $r_2(K)$ 是 K 的复素位的个数而 $\delta_p(K)\geqslant 0$ 是 K 在 p 处的 Leopoldt 缺陷. Leopoldt 猜想即为 $\delta_p(K)=0$ 对于所有 p 和 K 成立, 它在 $K/\mathbb{Q}$ 是 Abel 扩张情形时已经得到证明. 称 $\mathrm{Gal}(M/K)$ 的 $\mathbb{Z}_p$- 扭子群为 K 的 $\mathcal{T}_p$- 群, 记为 $\mathcal{T}_p(K)$. 这是一个有限 Abel p 群.

Coates 和 Gras 等对于 $\mathcal{T}_p$- 群做了很多详细研究工作. Gras[8] 给出如下猜想:

猜想 2.1 (Gras 猜想) 任意数域 K 对于充分大的素数 p 都是 p- 有理的, 即当 p 充分大时, $\mathcal{T}_p(K)$ 是平凡的.

Coates 在 K 是全实域时, 证明了 $\mathcal{T}_p(K)$ 的阶的如下公式 (参见文献 [6], [7, III 2.6.5] 和 [8]), 进而通过 p- 进类数公式建立了 $\mathcal{T}_p(K)$ 与 p- 进 zeta 函数的联系.

定理 2.1 (Coates 阶公式) 设 $K\neq\mathbb{Q}$ 是全实域. 若 Leopoldt 猜想对于 (p,K) 成立, 即 $\delta_p(K)=0$, 则有

$$|\mathcal{T}_p(K)|=(p\text{- 进单位})\cdot\frac{p\cdot[K\cap\mathbb{Q}^{p,\mathrm{cyc}}:\mathbb{Q}]\cdot h(K)\cdot R_p(K)}{\sqrt{D_K}\cdot\prod_{\mathfrak{p}\,|\,p}N\mathfrak{p}},\tag{2.1}$$

这里 $h(K)$ 是 K 的类数, $R_p(K)$ 是 p- 进调整子, D_K 是 K 的判别式, $\mathbb{Q}^{p,\mathrm{cyc}}$ 是 $\mathbb{Q}$ 的分圆 $\mathbb{Z}_p$- 扩张, 而乘积过 K 中位于 p 上的所有素理想, N 是 K 到 $\mathbb{Q}$ 的范映射.

更进一步地, 文献 [7, III 2.6.1] 还发现了适用于一般数域的更复杂的阶公式, 本文不需要这个公式.

Gras 给出了一般数域 $\mathcal{T}_p$- 群的 p- 秩公式. 设 $\mathrm{Cl}(\mathcal{O}_{K(\mu_p)}[\frac{1}{p}])$ 和 $\mathrm{Cl}^+(\mathcal{O}_{K(\mu_p)}[\frac{1}{p}])$ 分别是 $K(\mu_p)$ 的 p- 整数环 $\mathcal{O}_{K(\mu_p)}[\frac{1}{p}]$ 的常义和狭义类群. 群 $\mathrm{Cl}(\mathcal{O}_{K(\mu_p)}[\frac{1}{p}])\otimes\mathbb{F}_p$ 是 $\mathbb{F}_p[\mathrm{Gal}(K(\mu_p)/K)]$- 模. 设 ψ 是分圆同态 $\mathrm{Gal}(K(\mu_p)/K)\to\mathbb{F}_p^\times$, $\mathrm{Cl}(\mathcal{O}_{K(\mu_p)}[\frac{1}{p}])^\psi$ 是 $\mathrm{Cl}(\mathcal{O}_{K(\mu_p)}[\frac{1}{p}])\otimes\mathbb{F}_p$ 的 ψ- 根子空间.

定理 2.2 (Gras p- 秩公式)　设 $g(K)$ 是 K 中位于 p 之上且在 $K(\mu_p)$ 中完全分裂的素理想个数. 若 $K\supseteq\mu_p$, 记 $\nu(K)=1$; 否则记 $\nu(K)=0$, 则

$$\mathrm{rk}_p\mathcal{T}_p(K)=g(K)-\nu(K)-\delta_p(K)+\begin{cases}\mathrm{rk}_p\left(\mathrm{Cl}\left(\mathcal{O}_{K(\mu_p)}\left[\frac{1}{p}\right]\right)^\psi\right), & \text{若 } p\neq 2,\\ \mathrm{rk}_2\left(\mathrm{Cl}^+\left(\mathcal{O}_K\left[\frac{1}{2}\right]\right)\right), & \text{若 } p=2.\end{cases}\tag{2.2}$$

2.2 Pitoun-Vareson 定理

基于下面的结果, Pitoun 和 Varescon [4] 发展了一套算法来计算 $\mathcal{T}_p(K)$ 并研究 p- 有理的数域的比值:

定理 2.3 (Pitoun-Varescon)　设 $\mathcal{A}_{p^n}(K)$ 是 K 的模 p^n 的射影类群的 p 部分. 设 $e=\max_{\mathfrak{p}\mid p}\{e_\mathfrak{p}\}$ 是 p 在 $K/\mathbb{Q}$ 上的最大分歧次数. 设 Leopoldt 猜想对于 K 在 p 处成立, 则存在整数

$$n\geqslant 2+\nu_p(e), w, a_1,\ldots,a_{r_2(K)+1}, b_1,\ldots,b_w$$

使得

$$\mathcal{A}_{p^n}(K)\cong\prod_{i=1}^{w}\mathbb{Z}/b_i\mathbb{Z}\times\prod_{j=1}^{r_2(K)+1}\mathbb{Z}/a_j\mathbb{Z}$$

满足条件 $\min(\nu_p(a_j))\geqslant\max(\nu_p(b_i))+2$, 且

$$\mathcal{A}_{p^{n+1}}(K)\cong\prod_{i=1}^{w}\mathbb{Z}/b_i\mathbb{Z}\times\prod_{j=1}^{r_2(K)+1}\mathbb{Z}/pa_j\mathbb{Z}.$$

更进一步地, 有

$$\mathcal{T}_p(K)\cong\prod_{i=1}^{w}\mathbb{Z}/b_i\mathbb{Z}.$$

2.3 二次域的 $\mathcal{T}_2$- 群

对于无平方因子整数 m, 记 $\mathcal{T}_p(m)=\mathcal{T}_p(\mathbb{Q}(\sqrt{m}))$. 如引言所述, $\mathcal{T}_2$- 群与实二次域基本单位的迹联系密切.

命题 2.1　设 $l\equiv\pm1\pmod 8$ 是素数, $\varepsilon_l=a_l+b_l\sqrt{l}$ 是 $\mathbb{Q}(\sqrt{l})$ 的基本单位, 则

$$\nu_2(|\mathcal{T}_2(l)|)=\nu_2(L_2(1,\chi_l))-1=\nu_2(a_l)-1.$$

证明　设 $K=\mathbb{Q}(\sqrt{l})$. 此时 2- 进调整子 $R_2(K)$ 等于 $\log_2(\varepsilon_l)$. 由 2- 进类数公式 (参见文献 [9, 定理 5.24]) 可得

$$\frac{2h(K)\log_2(\varepsilon_l)}{\sqrt{D_K}}=\left(1-\frac{\chi_l(2)}{2}\right)^{-1}\cdot L_2(1,\chi_l),$$

又由于 $2\nmid h(K)$, 因此有 $\nu_2(L_2(1,\chi_l))=\nu_2(\log_2(\varepsilon_l))$. 这样第一个等式由定理 2.1 即得. 接下来需要证明 $\nu_2(\log_2(\varepsilon_l))=\nu_2(a_l)$.

若 $l\equiv 1\pmod 8$, 容易看出 a_l 和 b_l 是整数. 又由于此时 $N(\varepsilon_l)=\varepsilon_l\bar{\varepsilon}_l=-1$, 即 $a_l^2-lb_l^2=-1$, 因此 $4\mid a_l$ 且 b_l 是奇数. 故 $\nu_2(\varepsilon_l^2-1)=\nu_2(\varepsilon_l^2+\varepsilon_l\bar{\varepsilon}_l)=1+\nu_2(a_l)\geqslant 3$. 这说明

$$\nu_2(\log_2(\varepsilon_l^2))=\nu_2(\varepsilon_l^2-1)=1+\nu_2(a_l).$$

若 $l\equiv -1\pmod 8$, 此时 $2\mid a_l$ 且 b_l 是奇数 (参见文献 [10]). 这样有

$$\nu_2(\varepsilon_l^4-1)=\nu_2(\varepsilon_l^4-\varepsilon_l^2\bar{\varepsilon}_l{}^2)=2+\nu_2(a).$$

因此对于 $l\equiv\pm 1\pmod 8$, 也有 $\nu_2(\log_2(\varepsilon_l))=\nu_2(a_l)$. □

由 Gras 的 p- 秩公式, 可得二次域 $\mathcal{T}_2$- 群的 2- 秩.

命题 2.2 设 m 是有 t 个奇素因子的无平方因子整数, 则

$$\mathrm{rk}_2\mathcal{T}_2(m)=\begin{cases}t, & \text{若 } m \text{ 的所有奇素因子}\equiv\pm 1\pmod 8,\\ t-1, & \text{若存在 } m \text{ 的奇素因子}\equiv\pm 3\pmod 8.\end{cases}$$

证明 设 S 是 $K=\mathbb{Q}(\sqrt{m})$ 中位于 2 上的素理想集合. 记 $\mathrm{Cl}^+(K)$ 是 K 的狭义理想类群. 由于 Leopoldt 猜想于对二次域成立, 由定理 2.2, 可得

$$\mathrm{rk}_2\mathcal{T}_2(m)=|S|-1+\left|\frac{\mathrm{Cl}^+(K)}{2\mathrm{Cl}^+(K)+\langle S\rangle}\right|,$$

这里 $\langle S\rangle$ 是 $\mathrm{Cl}^+(K)$ 中由 S 生成的子群. 考虑正合列

$$0\longrightarrow\frac{\langle S\rangle}{2\mathrm{Cl}^+(K)\cap\langle S\rangle}\longrightarrow\frac{\mathrm{Cl}^+(K)}{2\mathrm{Cl}^+(K)}\longrightarrow\frac{\mathrm{Cl}^+(K)}{2\mathrm{Cl}^+(K)+\langle S\rangle}\longrightarrow 0.$$

首先由亏格理论可知, 中间项的 2- 秩是分歧素数的个数 -1. 故第三项的 2- 秩由第一项的 2- 秩给出.

为计算第一项的 2- 秩, 我们使用 Gauss 的一个定理: 理想 $\mathfrak{a}$ 在 $\mathrm{Cl}^+(K)$ 中是平方元当且仅当 $N\mathfrak{a}:=|O_K/\mathfrak{a}|\in N(K^\times)$. (证明: $\Rightarrow$ 是平凡的. 反过来假设 $N\mathfrak{a}=N(x)$, $x\in K$. 由于 $N\mathfrak{a}>0$, x 全正或者全负. 将 x 由 $\mathrm{sgn}(x)x$ 代替, 可以假设 x 全正. 由于 $H^1(\mathrm{Gal}(K/\mathbb{Q}),I_K)$ 平凡, 这里 I_K 是 K 的分式理想群, 故 $(x)^{-1}\mathfrak{a}=\mathfrak{b}^\sigma/\mathfrak{b}$ 对于某个 $\mathfrak{b}\in I_K$ 成立, 其中 $1\neq\sigma\in\mathrm{Gal}(K/\mathbb{Q})$. 再由 $\mathrm{Cl}^+(K)^{1-\sigma}=2\mathrm{Cl}^+(K)$ 即得结论.) Gauss 的定理给出

$$[\langle S\rangle:2\mathrm{Cl}^+(K)\cap\langle S\rangle]=\begin{cases}1, & \text{若 } m\equiv 5\pmod 8 \quad \text{或} \quad 2\in N(K^\times),\\ 2, & \text{其他情形.}\end{cases}$$

这样 2- 秩公式只需对 m 的所有奇素因子 p 讨论 $p\pmod 8$ 即得. □

推论 2.1 (1) 若素数 $l\equiv\pm 1\pmod 8$, 则 $\mathrm{rk}_2(\mathcal{T}_2(\pm l))=\mathrm{rk}_2(\mathcal{T}_2(\pm 2l))=1$;

(2) 若 m 是无平方因子正整数且 $\mathbb{Q}(\sqrt{-m})$ 的分圆岩泽不变量 $\lambda(-m)$ 等于 1, 则 $\mathrm{rk}_2(\mathcal{T}_2(m))=1$.

证明 (1) 由命题 2.2 直接给出.

(2) 由木田公式 (参见文献 [5, 推论 1]) 可知, $\lambda(-m)=1$ 当且仅当 m 或 $\frac{m}{2}$ 要么是素数 p 且 $p\equiv\pm 7\pmod{16}$, 要么是素数 p 和 q 的乘积 pq 且 $p=q\equiv\pm 3\pmod 8$. 故由命题 2.2 即得推论成立. □

3 Cohen-Lenstra 猜想

Cohen-Lenstra 猜想, 泛而言之, 即预测某些自然产生的算术对象序列在某个权重空间中是均匀分布的, 而且算术对象的权重应该反比于它的自同构群的阶. 这方面最初思想源自 Cohen 和 Lenstra[11]. 他们使用这样类型的猜想来预测虚二次域和素数阶全实域的类群的分布. 现在, Cohen-Lenstra 猜想已经被推广到其他新的算术对象, 如椭圆曲线的 Selmer 群和 Shafarevich-Tate 群 (参见文献 [12,13]). 由于对于 $\mathcal{T}_p$- 群缺乏整体刻画, 我们将着眼于局部版本的 Cohen-Lenstra 猜想.

3.1 局部设定

令 A 是离散赋值环, π 是它的素元. 假设它的剩余类域 $k=A/\pi A$ 是 q 元有限域. 令 $\mathcal{M}_A$ 是所有有限 A- 模自同构类的集合, 在直和作为加法意义下, 它是一个含幺半群.

定义 3.1 对于有限 A- 模 G, 记 $\mathrm{Aut}_A(G)$ 为 G 的 A- 自同构群. 对于任意正整数 i, 记

$$\mathrm{rk}_{\pi^i}G := \dim_k \pi^{i-1}G/\pi^i G$$

是 G 的 π^i- 秩.

由主理想整环上有限生成模的结构定理, 可得

$$G \cong \prod_i (A/\pi^i A)^{a_i}, \quad a_i = 0 \text{ 对于几乎所有的 } i \text{ 成立.}$$

此时有

$$|G| = q^{\sum_i ia_i}, \quad \mathrm{rk}_\pi G = \sum_i a_i. \tag{3.1}$$

定义 3.2 $\mathcal{M}_A$ 上的一个权重函数即映射 $\omega : \mathcal{M}_A \longrightarrow \mathbb{R}_{\geqslant 0}$.

例 3.1 对于非负整数 u, 权重函数 ω_u 如下定义:

$$\omega_u(G) := \frac{1}{|G|^u \cdot |\mathrm{Aut}_A(G)|}. \tag{3.2}$$

对于类群和 $\mathcal{T}_p$- 群的 Cohen-Lenstra 猜想, 我们将着重使用 ω_0 和 ω_1.

定义 3.3 固定 $\mathcal{M}_A$ 上的权重 ω. $\mathcal{M}_A$ 的子集合 V 上的复值函数 f 称为关于权重 ω 的 L^1- 函数是指

$$\lim_{N\to\infty} \sum_{\substack{G\in V,\\ |G|\leqslant N}} |f(G)|\omega(G) < \infty$$

成立. 对于这样的 f, 它的 ω- 加权均值定义为

$$M(f,V,\omega) := \lim_{N\to\infty} \frac{\sum_{G\in V,|G|\leqslant N} f(G)\omega(G)}{\sum_{G\in V,|G|\leqslant N} \omega(G)}.$$

例 3.2 特征函数 1_V 是 V 上关于权重 ω_u 的 L^1- 函数. 由命题 3.1(2) 可知

$$\sum_{G\in V} \omega_u(G) \leqslant \sum_{G\in\mathcal{M}_A} \omega_u(G)$$

总是有限值.

命题 3.1 设 $\mathcal{M}_r$ 和 $\mathcal{M}^0$ 分别是 $\mathcal{M}_A$ 中秩为 r 的模和非平凡模构成的同构类构成的子集合. 定义 $\eta_0(q)=1$ 且对于 $i\geqslant 1$,

$$\eta_i(q)=\eta_{i-1}(q)(1-q^{-i})=\prod_{j=1}^{i}(1-q^{-j}),$$

则极限 $\eta_\infty(q)=\lim_{i\to\infty}\eta_i(q)$ 收敛且有

(1)

$$M(1_{\mathcal{M}_r},\mathcal{M}_A,\omega_u)=\frac{\eta_\infty(q)}{q^{r(r+u)}\eta_r(q)\eta_{r+u}(q)};$$

(2)

$$\sum_{G\in\mathcal{M}_A}\omega_u(G)=\frac{\eta_u(q)}{\eta_\infty(q)}\quad 且\quad M(1_{\mathcal{M}^0},\mathcal{M}_A,\omega_u)=1-\frac{\eta_\infty(q)}{\eta_u(q)};$$

(3) 若 1_G 是有限 A- 模 G 的特征函数, 则

$$M(1_G,\mathcal{M}_A,\omega_u)=\frac{\eta_\infty(q)}{\eta_u(q)}\omega_u(G).$$

证明 (1) 参见文献 [11, 定理 6.3]. (2) 和 (3) 由 (1) 立得. □

命题 3.2 若 $A=\mathbb{Z}_p$, 则 $\mathcal{M}_{\mathbb{Z}_p}$ 是有限 Abel p- 群的同构类集合.

(1) 对于有限 Abel p- 群 G, 有

$$M(1_G,\mathcal{M}_{\mathbb{Z}_p},\omega_u)=\frac{\eta_\infty(p)}{\eta_u(p)}\omega_u(G);$$

(2) 设 $V_j=\{\mathbb{Z}/2^k\mathbb{Z}:k\geqslant j\}\subseteq\mathcal{M}_{\mathbb{Z}_2}$, 则对于 $k\geqslant 0$ 且 $j\geqslant 1$, 有

$$M(1_{\mathbb{Z}/2^{k+j}\mathbb{Z}},V_j,\omega_0)=\frac{1}{2^{k+1}}.$$

证明 (1) 是前述命题 (3) 的特殊情形. (2) 由直接计算即得. □

定义 3.4 设 ω 是 $\mathcal{M}_A$ 的权重函数. $\mathcal{M}_A$ 中的序列 $\{M_i\}_{i\geqslant 1}$ 称为关于 (V,ω) 均匀分布是指 $V=\bigcup\{M_i\}\subseteq\mathcal{M}_A$ 是它的上域, 且等式

$$\lim_{n\to\infty}\frac{\sum_{i=1}^{n}f(M_i)}{n}=M(f,V,\omega)$$

对于 V 上所有关于 ω 的 L^1 函数 f 均成立.

我们以两个注记来结束本小节.

注 3.1 与 Cohen 和 Lenstra [11] 的原始设定比较而言, 我们的设定有两处不同.

(1) 对于均匀分布的原始设定, Cohen 和 Lenstra 使用的是 "合理的" 函数, 而不是 L^1 函数, 但在他们原始文章中并没有给出 "合理的" 的确切定义. Cohen 和 Lenstra 建议 "合理的" 函数可能包括所有非负值函数, 但这可能会引起一些收敛性的问题. Friedman 和 Washington 在文献 [14, 注 3] 中建议 "合理的" 函数可能就是所有 L^1 函数, Bhargava 等 [12] 的一个想法是所有实值 L^1 函数是 "合理的". Bartel 和 Lenstra Jr 在最新的文献 [15] 中, 建议考虑满足对于任意 $j\geqslant 1$, f^j 都是 L^1 函数的 f.

(2) Cohen 和 Lenstra 最开始的猜想是整体性的, 即 A 是 Dedekind 环而不是离散赋值环. 一般而言, 对于权重函数 ω_u, 局部猜想比整体猜想要弱一些. 对于有限 A- 模 G 和 A 的任意素理想 $\mathfrak{p}$, G 的 $\mathfrak{p}$- 准素部分 $G(\mathfrak{p})$ 是有限 $A_\mathfrak{p}$- 模, 并且 $|G|=\prod_\mathfrak{p}|G(\mathfrak{p})|$ 和 $|\mathrm{Aut}_A(G)|=\prod|\mathrm{Aut}_{A_\mathfrak{p}}(G(\mathfrak{p}))|$. 如果 f 是 $\mathcal{M}_{A_\mathfrak{p}}$

上的 ω_u 相关的 "合理的" 函数, 则可将 f 视为 $\mathcal{M}_A$ 上关于 ω_u 的 "合理的" 函数 $\widetilde{f}: G \mapsto f(G(\mathfrak{p}))$. 由文献 [11, 命题 5.7] 知,

$$M(\widetilde{f}, \mathcal{M}_A, \omega_u) = M(f, \mathcal{M}_{A_\mathfrak{p}}, \omega_u).$$

因此, 如果序列 $\{G_i\}$ 在 $(\mathcal{M}_A, \omega_u)$ 上均匀分布, 那么 $\{G_i(\mathfrak{p})\}$ 在 $(\mathcal{M}_{A_\mathfrak{p}}, \omega_u)$ 上也是均匀分布.

注 3.2 对于 Shafarevich-Tate 群的情形 (参见文献 [12, 16]), 上述设定需要做一些变化. 有限 Abel p- 群称为辛 p- 群 (辛 $\mathbb{Z}_p$- 模), 是指 G 上具备非退化反对称配对 $[\cdot,\cdot]: G \times G \to \mathbb{Q}_p/\mathbb{Z}_p$. 所有辛 p- 群的同构类 $\mathcal{M}_A^s$ (此处同构须保持辛结构) 是一个含幺半群. G 的 u- 权重函数现在定义为 $\omega_u^s(G) = \frac{1}{|G|^u \cdot |\mathrm{Aut}^s(G)|}$, 这里 $\mathrm{Aut}^s(G)$ 是 G 保持辛结构的自同构群. 这样同样有关于 (V, ω_u^s) 均匀分布的概念.

3.2 类群的局部 Cohen-Lenstra 猜想

本小节回顾类群的局部 Cohen-Lenstra 猜想. 设 $\mathcal{F}_{\mathrm{im}}$ 是所有虚二次域组成的集合族, 由它们的判别式的绝对值排序. 对于素数 ℓ, 记 $\mathcal{F}_{\mathrm{re},\ell}$ 是有理数域的 ℓ- 次循环全实扩张组成的集合族, 由判别式排序. 特别地, $\mathcal{F}_{\mathrm{re}} = \mathcal{F}_{\mathrm{re},2}$ 是全体实二次域构成的集合族. 令 $\mathrm{Cl}_p^+(K)$ 是 K 的狭义类群的 p- 部分. 对于 $K \in \mathcal{F}_{\mathrm{re},\ell}$, 令 σ 是 $\mathrm{Gal}(K/\mathbb{Q})$ 的一个生成元. 狭义类群 $\mathrm{Cl}^+(K)$ 作为 $\mathbb{Z}[\mathrm{Gal}(K/\mathbb{Q})]$- 模, $N_G := 1 + \sigma + \cdots + \sigma^{\ell-1}$ 在其上作用平凡, 因此它可以看作 $\mathbb{Z}[\mathrm{Gal}(K/\mathbb{Q})]/(N_G)$- 模. 注意到 $\mathbb{Z}[\mathrm{Gal}(K/\mathbb{Q})]/(N_G) \cong \mathbb{Z}[\zeta_\ell]$, 其中 $\sigma \mapsto \zeta_\ell$. 若 $\mathfrak{p}$ 是 $\mathbb{Z}[\zeta_\ell]$ 中位于 p 上的一个素理想, 记 $\mathrm{Cl}_\mathfrak{p}^+(K)$ 为 $\mathrm{Cl}^+(K)$ 的 $\mathfrak{p}$- 准素部分, 则它是 $\mathbb{Z}[\zeta_\ell]_\mathfrak{p}$- 模, 此处 $\mathbb{Z}[\zeta_\ell]_\mathfrak{p}$ 是 $\mathbb{Z}[\zeta_\ell]$ 在 $\mathfrak{p}$ 处的完备化.

猜想 3.1 (Cohen-Lenstra-Gerth III, 局部版本) (1) 虚二次域情形: $\mathbb{Z}_p$- 模序列 $\{2\mathrm{Cl}_p(K)\}_{K\in\mathcal{F}_{\mathrm{im}}}$ 关于 $(\mathcal{M}_{\mathbb{Z}_p}, \omega_0)$ 均匀分布.

(2) 实二次域情形: $\mathbb{Z}_p$- 模序列 $\{2\mathrm{Cl}_p^+(K)\}_{K\in\mathcal{F}_{\mathrm{re}}}$ 关于 $(\mathcal{M}_{\mathbb{Z}_p}, \omega_1)$ 均匀分布.

(3) 全实奇素数扩张情形: 设 ℓ 和 p 是奇素数. 设 $\mathfrak{p}$ 是 $\mathbb{Z}[\zeta_\ell]$ 中位于 p 上的一个素理想, 则 $\mathbb{Z}[\zeta_\ell]_\mathfrak{p}$- 模序列 $\{(1-\zeta_\ell)\mathrm{Cl}_\mathfrak{p}^+(K)\}_{K\in\mathcal{F}_{\mathrm{re},\ell}}$ 关于 $(\mathcal{M}_{\mathbb{Z}[\zeta_\ell]_\mathfrak{p}}, \omega_1)$ 均匀分布.

最初形式的 Cohen-Lenstra 猜想是关于狭义类群的与 ℓ 互素部分的一个整体性的猜想, 对于 ℓ- 部分的改进参见文献 [17]. 当 ℓ 是奇数时, Malle[18] 发现了位于 2 上的素理想也是坏的, 并在 Gerth III[19] 的结果的启发下提出了改进的预测. 接下来, Cohen 和 Martinet[20–22] 将猜想推广到基域是一般数域的情形. 这里不考虑一般情形, 因为需要剔除更多坏的素理想, 并作出更多改进. 粗略地, 对于基域 K, 实验数据揭示所有满足 $p \mid [K:\mathbb{Q}]$ 或 $\mu_p \subseteq K$ 的素数 p 都是坏的, 而大家普遍相信几乎所有的素数都是好的.

Park 等[13] 及 Friedman 和 Washington[14] 在有限域上曲线 Jacobi 簇类似结果的激励下, 使用随机矩阵理论重新解释了上面猜想的一些情形.

对于类群的局部 Cohen-Lenstra 猜想, 近年来有 3 个突破性的工作. 对于命题 3.1 中的函数 $1_{\mathcal{M}_r}$, Fouvry 和 Klüners 证明了下面的结论.

定理 3.1[23] 对于任意整数 $r \geqslant 0$, 有

$$\lim_{X\to\infty} \frac{\#\{K \in \mathcal{F}_{\mathrm{im}}, |D_K| \leqslant X,\ \mathrm{rk}_2\ 2\mathrm{Cl}_2(K) = r\}}{\#\{K \in \mathcal{F}_{\mathrm{im}}, |D_K| \leqslant X\}} = \frac{\eta_\infty(2)}{2^{r^2}\eta_r(2)^2},$$

$$\lim_{X\to\infty} \frac{\#\{K \in \mathcal{F}_{\mathrm{re}}, |D_K| \leqslant X,\ \mathrm{rk}_2\ 2\mathrm{Cl}_2^+(K) = r\}}{\#\{K \in \mathcal{F}_{\mathrm{re}}, |D_K| \leqslant X\}} = \frac{\eta_\infty(2)}{2^{r(r+1)}\eta_r(2)\eta_{r+1}(2)}.$$

对于任意 G 的特征函数 1_G 的加权均值, Smith 和 Koymans-Pagano 分别给出如下结果:

定理 3.2 [24] 对于任意有限 Abel 2- 群 G, 总有

$$\lim_{X\to\infty}\frac{\#\{K\in\mathcal{F}_{\rm im},|D_K|\leqslant X,\ 2{\rm Cl}_2(K)\cong G\}}{\#\{K\in\mathcal{F}_{\rm im},|D_K|\leqslant X\}}=\frac{\eta_\infty(2)}{|{\rm Aut}(G)|}.$$

注 3.3 (1) 事实上, Smith 得到了关于 2- 类群秩的随机分布结果, 这个定理是自然推论.

(2) 正如 Wood [25] 所言, 由于涉及求和与求极限的次序交换, 单纯从定理 3.2 的叙述不能直接推导出 Fouvry-Klüners 的定理 3.1.

定理 3.3 [26] 假设广义 Riemann 假设 (GRH) 成立. 设 ℓ 是奇素数, 则对于有限 $\mathbb{Z}_\ell[\zeta_\ell]$- 模 G, 有

$$\lim_{X\to\infty}\frac{\#\{K\in\mathcal{F}_{{\rm re},\ell},{\rm rad}(D_K)<X,\ (1-\zeta_\ell){\rm Cl}^+_{(1-\zeta_\ell)}(K)\cong G\}}{\#\{K\in\mathcal{F}_{{\rm re},\ell},\ {\rm rad}(D_K)<X\}}=\frac{\eta_\infty(l)/\eta_1(l)}{|G||{\rm Aut}_{\mathbb{Z}_\ell[\zeta_\ell]}(G)|},$$

这里 ${\rm rad}(D_K)$ 是 D_K 的所有素因子的乘积.

3.3 虚二次域 2- 类群的扩展 Cohen-Lenstra 猜想

本小节给出类群在虚二次域子集合族上的扩展猜想. 这些猜想的隐性形式在文献 [5, 27–31] 可以找到, 特别地, 文献 [5, 第 1253 页] 将它视为 Cohen-Lenstra 猜想的扩展形式. 我们将给出明确的形式, 并在下节对于 $\mathcal{T}_p$- 群提出类比的扩展形式.

首先回忆记号. 对于无平方因子整数 m, ${\rm Cl}_2(m)$、$h_2(m)$ 和 $h(m)$ 分别是 $\mathbb{Q}(\sqrt{m})$ 的 2- 类群、2- 类数和类数. 集合 $V_j=\{\mathbb{Z}/2^k\mathbb{Z}:k\geqslant j\}$ 是 $\mathcal{M}_{\mathbb{Z}_2}$ 的子集合. 注意到, 如果 G 是 2- 循环群, $G\in V_j$ 即为 $|G|\geqslant 2^j$.

由 Gauss 的亏格理论和 Rédei 矩阵理论 (参见文献 [32], 特别是文献 [33], ${\rm Cl}_2(-2l)$ 的证明参见文献 [34, 定理 4.2]), 我们有下面的命题.

命题 3.3 设 l 是奇素数. ${\rm Cl}_2(-l)$ 和 ${\rm Cl}_2(-2l)$ 均是循环群.

(1) 若 $l\equiv 3\pmod 4$, 则 $h_2(-l)=1$; 若 $l\equiv 5\pmod 8$, 则 $h_2(-l)=2$; 若 $l\equiv 1\pmod 8$, 则 $h_2(-l)\geqslant 4$. 更进一步地, 若 $l\equiv 1\pmod 8$, 设 $l=2g^2-h^2$, 则 $h_2(-l)=4$ 当且仅当 $g\equiv 3\pmod 4$, $h_2(-l)=8$ 当且仅当 $(\frac{2h}{g})(\frac{g}{l})_4=-1$.

(2) 若 $l\equiv\pm 3\pmod 8$, 则 $h_2(-2l)=2$; 若 $l\equiv\pm 1\pmod 8$, 则 $h_2(-2l)\geqslant 4$. 更进一步地,

(i) 若 $l\equiv 1\pmod 8$, 设 $l=u^2-2v^2$ 且 $u\equiv 1\pmod 4$, 则 $h_2(-2l)=4$ 当且仅当 $u\equiv 5\pmod 8$, $h_2(-2l)=8$ 当且仅当 $(\frac{u}{l})_4=-1$.

(ii) 若 $l\equiv 7\pmod 8$, 则 $h_2(-2l)=4$ 当且仅当 $l\equiv 7\pmod{16}$, $h_2(-2l)=8$ 当且仅当 $l\equiv 15\pmod{16}$ 且 $(-1)^{\frac{l+1}{16}}(\frac{2u}{v})=-1$, 这里 $(u,v)\in\mathbb{Z}^2_{>0}$ 满足条件 $l=u^2-2v^2$.

猜想 3.2 序列 $\{{\rm Cl}_2(-l)\}_{l\equiv 1\ (\rm mod\ 8)}$、$\{{\rm Cl}_2(-2l)\}_{l\equiv 1\ (\rm mod\ 8)}$ 和 $\{{\rm Cl}_2(-2l)\}_{l\equiv -1\ (\rm mod\ 8)}$ 关于 (V_2,ω_0) 都是均匀分布.

特别地, 对于非负整数 k, 取特征函数 $1_{\mathbb{Z}/2^{k+2}\mathbb{Z}}$, 则有

$$\lim_{X\to\infty}\frac{\#\{l\leqslant X:l\equiv 1\ (\rm mod\ 8)\ 且\ {\rm Cl}_2(-l)\cong\mathbb{Z}/2^{k+2}\mathbb{Z}\}}{\#\{l\leqslant X:l\equiv 1\ (\rm mod\ 8)\}}=\frac{1}{2^{k+1}},\tag{3.3}$$

$$\lim_{X\to\infty}\frac{\#\{l\leqslant X:l\equiv 1\ (\rm mod\ 8),{\rm Cl}_2(-2l)\cong\mathbb{Z}/2^{k+2}\mathbb{Z}\}}{\#\{l\leqslant X:l\equiv 1\ (\rm mod\ 8)\}}=\frac{1}{2^{k+1}},\tag{3.4}$$

$$\lim_{X\to\infty}\frac{\#\{l\leqslant X:l\equiv -1\ (\rm mod\ 8),{\rm Cl}_2(-2l)\cong\mathbb{Z}/2^{k+2}\mathbb{Z}\}}{\#\{l\leqslant X:l\equiv -1\ (\rm mod\ 8)\}}=\frac{1}{2^{k+1}}.\tag{3.5}$$

注 3.4 Milovic [29] 首先猜测等式 (3.3) 成立. 猜想中的 3 个等式在 $k=0$ 和 $k=1$ 情形已得到证明. Stevenhagen [30,31] 的工作说明类群 $\mathrm{Cl}_2(-l)$ 和 $\mathrm{Cl}_2(-2l)$ 的 8- 秩只依赖于 l 在对应的监管域 (governing field) 上的分裂情形 (参见定理 3.4 的证明), 这样就得到 $k=0$ 的情形. 基于文献 [33] 中 $\mathrm{Cl}_2(-l)$ 和 $\mathrm{Cl}_2(-2l)$ 的 16- 秩的结果, 文献 [27–29] 证明了 $k=1$ 的情形.

猜想 3.3 序列 $\{\mathrm{Cl}_2(-l)\}_{l\equiv 9 \pmod{16}}$ 和 $\{\mathrm{Cl}_2(-2l)\}_{l\equiv 9 \pmod{16}}$ 关于 (V_2,ω_0) 是均匀分布.

注 3.5 猜想 3.2 和 3.3 一起说明序列 $\{\mathrm{Cl}_2(-l)\}_{l\equiv 1 \pmod{16}}$ 和 $\{\mathrm{Cl}_2(-2l)\}_{l\equiv 1 \pmod{16}}$ 关于 (V_2,ω_0) 也是均匀分布.

取特征函数 $1_{\mathbb{Z}/2^{k+2}\mathbb{Z}}$, 猜想 3.3 说明下面两个等式成立:

$$\lim_{X\to\infty}\frac{\#\{l\leqslant X: l\equiv 9 \pmod{16}, \mathrm{Cl}_2(-l)\cong \mathbb{Z}/2^{k+2}\mathbb{Z}\}}{\#\{l\leqslant X: l\equiv 9 \pmod{16}\}}=\frac{1}{2^{k+1}}, \tag{3.6}$$

$$\lim_{X\to\infty}\frac{\#\{l\leqslant X: l\equiv 9 \pmod{16}, \mathrm{Cl}_2(-2l)\cong \mathbb{Z}/2^{k+2}\mathbb{Z}\}}{\#\{l\leqslant X: l\equiv 9 \pmod{16}\}}=\frac{1}{2^{k+1}}. \tag{3.7}$$

根据文献 [27,29] 的方法, 我们有下面的定理.

定理 3.4 猜想 1.1 中的等式 (1.1) 与 (3.6) 等价. 在 $k=0$ 和 $k=1$ 情形, 两等式成立.

证明 等价性如引言所述.

Koymans [27] 证明了 (3.3) 的 $k=1$ 情形, 即

$$\lim_{X\to\infty}\frac{\#\{l\leqslant X: l\equiv 1 \pmod 8 \text{ 且 } 8\mid h(-l)\}}{\#\{l\leqslant X: l\equiv 1 \pmod 8\}}=\frac{1}{4}.$$

由文献 [31], $l\equiv 9 \pmod{16}$ 且 $h_2(-l)\geqslant 8$ 当且仅当 l 在 $\mathrm{Gal}(\mathbb{Q}(\zeta_{16},\sqrt{1+\mathrm{i}})/\mathbb{Q})$ 的 Frobenius 限制在 $\mathbb{Q}(\zeta_8,\sqrt{1+\mathrm{i}})$ 上平凡且将 ζ_{16} 映到 $-\zeta_{16}$. 由 Chebatarev 密度定理, $k=0$ 得证, 即

$$\lim_{X\to\infty}\frac{\#\{l\leqslant X: l\equiv 9 \pmod{16}, 8\mid h(-l)\}}{\#\{l\leqslant X: l\equiv 9 \pmod{16}\}}=\lim_{X\to\infty}\frac{\#\{l\leqslant X: l\equiv 1 \pmod{16}, 8\mid h(-l)\}}{\#\{l\leqslant X: l\equiv 1 \pmod{16}\}}=\frac{1}{2}.$$

如果

$$\lim_{X\to\infty}\frac{\#\{l\leqslant X: l\equiv 9 \pmod{16}, 8\parallel h(-l)\}}{\#\{l\leqslant X: l\equiv 9 \pmod{16}\}}=\lim_{X\to\infty}\frac{\#\{l\leqslant X: l\equiv 9 \pmod{16}, 16\mid h(-l)\}}{\#\{l\leqslant X: l\equiv 9 \pmod{16}\}}=\frac{1}{4}, \tag{3.8}$$

则

$$\lim_{X\to\infty}\frac{\#\{l\leqslant X: l\equiv 1 \pmod{16}, 16\mid h(-l)\}}{\#\{l\leqslant X: l\equiv 1 \pmod{16}\}}=\lim_{X\to\infty}\frac{\#\{l\leqslant X: l\equiv 1 \pmod{16}, 8\parallel h(-l)\}}{\#\{l\leqslant X: l\equiv 1 \pmod{16}\}}=\frac{1}{4}.$$

即 $k=1$ 的情形得证. 因此只需证 (3.8).

令

$$e_l=\begin{cases}1, & \text{若 } 16\mid h(-l),\\ -1, & \text{若 } 8\parallel h(-l),\\ 0, & \text{若 } 4\parallel h(-l).\end{cases}$$

文献 [27] 证明了

$$\sum_{l\leqslant X,\ l\equiv 1 \pmod 8} e_l\ll\frac{X}{\exp((\log X)^{0.1})}. \tag{3.9}$$

对于所有 $\mathbb{Z}[\zeta_8]$ 中的全正元 w, 如果将文献 [27, 引理 4.1 和 4.2] 中的旋量符号 $[w]$ 由扭曲旋量符号 $[w]' := [w]\cdot\lambda(w)$ 代替, 其中若 $Nw\equiv 1 \pmod 8$, 则定义 $\lambda(w)=(-1)^{\frac{Nw-1}{8}}$, 否则 $\lambda(w)=1$. 按照文献 [27] 中的论证即得

$$\sum_{l\leqslant X,\ l\equiv 1 \pmod 8} (-1)^{\frac{l-1}{8}} e_l \ll \frac{X}{\exp((\log X)^{0.1})}. \tag{3.10}$$

因此

$$\sum_{l\leqslant X, l\equiv 1 \pmod 8} (e_l - (-1)^{\frac{l-1}{8}} e_l) = 2 \sum_{l\leqslant X, l\equiv 9 \pmod{16}} (1_{16\,|\,h(-l)} - 1_{8\,\|\,h(-l)}) \ll \frac{X}{\exp((\log X)^{0.1})}.$$

若 $X\to+\infty$, 则 $\log X = o(\exp((\log X)^{0.1}))$, Dirichlet 密度定理告诉我们

$$\#\{l\leqslant X,\ l\equiv 9 \pmod{16},\ 8\,\|\,h(-l)\} \sim \#\{l\leqslant X,\ l\equiv 9 \pmod{16},\ 16\mid h(-l)\} \sim \frac{X}{32\log X}.$$

故 (3.8) 得证. □

注 3.6 由同样的方法, Li 和 Xu [34] 证明了如下结果:

$$\begin{aligned}&\lim_{X\to\infty} \frac{\#\{l\leqslant X : l\equiv 15 \pmod{32} \text{ 且 } \mathrm{Cl}_2(-2l)\cong\mathbb{Z}/8\mathbb{Z}\}}{\#\{l\leqslant X : l\equiv 15 \pmod{32}\}}\\ &= \lim_{X\to\infty} \frac{\#\{l\leqslant X : l\equiv 31 \pmod{32} \text{ 且 } \mathrm{Cl}_2(-2l)\cong\mathbb{Z}/8\mathbb{Z}\}}{\#\{l\leqslant X : l\equiv 31 \pmod{32}\}}\\ &= \frac{1}{2}.\end{aligned}$$

4 二次域 $\mathcal{T}$- 群分布的 Cohen-Lenstra 猜想

本节将对虚二次域族和实二次域族的 $\mathcal{T}_p$- 群分布提出 Cohen-Lenstra 猜想. 对于二次域族的一些子集族, 我们对于它们的 $\mathcal{T}_2$- 群分布提出扩展 Cohen-Lenstra 猜想. 我们还给出这些猜想的一些理论依据.

猜想 4.1 ($\mathcal{T}_p$- 群分布的 Cohen-Lenstra 猜想) 设 p 是素数.

(1) 虚二次域情形: $\mathbb{Z}_p$- 模序列 $\{6\mathcal{T}_p(K)\}_{K\in\mathcal{F}_{\mathrm{im}}}$ 关于 $(\mathcal{M}_{\mathbb{Z}_p},\omega_1)$ 均匀分布;

(2) 实二次域情形: $\mathbb{Z}_p$- 模序列 $\{6\mathcal{T}_p(K)\}_{K\in\mathcal{F}_{\mathrm{re}}}$ 关于 $(\mathcal{M}_{\mathbb{Z}_p},\omega_0)$ 均匀分布.

特别地, 对于有限 Abel p- 群 G, 有

$$\lim_{X\to\infty} \frac{\#\{K\in\mathcal{F}_{\mathrm{im}} \mid -D_K\leqslant X,\ 6\mathcal{T}_p(K)\cong G\}}{\#\{K\in\mathcal{F}_{\mathrm{im}} : -D_F\leqslant X\}} = \frac{\eta_\infty(p)/\eta_1(p)}{\#G\cdot\#\mathrm{Aut}(G)}, \tag{4.1}$$

$$\lim_{X\to\infty} \frac{\#\{K\in\mathcal{K}_{\mathrm{re}} \mid D_F\leqslant X,\ 6\mathcal{T}_p(K)\cong G\}}{\#\{K\in\mathcal{K}_{\mathrm{re}} : D_K\leqslant X\}} = \frac{\eta_\infty(p)}{\#\mathrm{Aut}(G)}. \tag{4.2}$$

注 4.1 注意到这里的权重函数与类群的权重函数恰好相反. 实际上, 如文献 [11, 第 8 节] 所说, 对于二次域的类群, 权重函数 ω_u 中出现的 u 恰好是单位群的 $\mathbb{Z}$- 秩. 根据 Gras 秩公式, $\mathcal{T}_p$- 群与 $\mathrm{Cl}(\mathcal{O}_{K(\mu_p)}[1/p])^\psi$ 关联, 因此我们的 u 应该是 $(\mathcal{O}_{K(\mu_p)}[1/p])^\times$ 的 ψ 部分的 p- 秩. 对于二次域 K 且 $p>3$, 根据文献 [35, 命题 8.1], 可得

$$u(K,p) := \mathrm{rk}_p((\mathcal{O}_{K(\mu_p)}[1/p])^\times)^\psi = \begin{cases} 0, & \text{若 } K \text{ 是实二次域,}\\ 1, & \text{若 } K \text{ 是虚二次域.}\end{cases}$$

这恰好与我们的数据一致.

对于这个猜想, 我们有几点说明:

(1) 对于 $p \geqslant 5$, 第 5 节关于 $p=5$ 和 $p=7$ 的数据以及 Pitoun 和 Varescon [4] 给出的数据都与猜想很吻合.

(2) 对于 $p=2$ 和 $p=3$ 的情形, 在界是 5×10^7 时, $2\mathcal{T}_2(K)$ 与 $3\mathcal{T}_3(K)$ 的分布其实不是很理想, 但这与 2- 类群分布的 Cohen-Lenstra 猜想出现的情形一样, 是可以预见的: 我们能够计算的界尚不够高, 还不能展现收敛情形. 至于更高的界, 需要更强的计算机. 我们的信心, 首先来自于 Smith [24] 关于 2- 类群的工作 (定理 3.2). 其次, 我们收集的数据表明, 对于 $p=2$ 或者 $p=3$, 满足 $p\mathcal{T}_p(D)\cong G$ 的基本判别式 D 的密度与 $\omega_1(G)$ (或者 $\omega_0(G)$) 的比值只与 G 的 p- 秩有关, 尽管与猜想略微不同, 但同样的现象在 2- 类群的数值中也会出现, 所以并非是某种反例. 最后, 对于虚二次域的 $\mathcal{T}_2$- 群, 基于 Gerth III [36]、Fouvry 和 Klüners [23] 以及 Yue 和 Yu [37] 的结果, 我们在文献 [38] 中证明了如下的秩密度公式, 这也是一个有力佐证.

定理 4.1 对于整数 $t\geqslant 1$ 和 $r\geqslant 0$ 以及实数 $x>0$, 令

$$\begin{aligned}
&N_x := \{m\in\mathbb{Z}_{>0} \mid m\leqslant x \text{ 无平方因子}\},\\
&N_{t;x} := \{m\in N_x \mid \text{ 恰好 } t \text{ 个素数在 } \mathbb{Q}(\sqrt{-m}) \text{ 中分歧}\},\\
&T^r_{t;x} := \{m\in N_{t;x} \mid \mathrm{rk}_2(2\mathcal{T}_2(\mathbb{Q}(\sqrt{-m}))) = r\},
\end{aligned}$$

则对于 $r\geqslant 0$, 如下定义的极限 $d^T_{\infty,r}$:

$$d^T_{\infty,r} := \lim_{t\to\infty}\lim_{x\to\infty}\frac{\#T^r_{t;x}}{\#N_{t;x}} \tag{4.3}$$

存在并且

$$d^T_{\infty,r} = \frac{\prod_{i=r+2}^{\infty}(1-2^{-i})}{2^{r(r+1)}\prod_{i=1}^{r}(1-2^{-i})} = \frac{\eta_\infty(2)}{2^{r(r+1)}\eta_r(2)\eta_{r+1}(2)}, \tag{4.4}$$

这里 $\eta_s(q) := \prod_{i=1}^{s}(1-q^{-i})$, 其中 $s\in\mathbb{Z}_{>0}\cup\{\infty\}$ 且 $q>1$ 以及 $\eta_0(q):=1$.

注 4.2 同类群情形一样, 正如 Wood [25] 所言, 暂时也不能由 $2\mathcal{T}_2(K)$ 关于特征函数分布的猜想 4.1 给出我们的 $\mathcal{T}_2$- 群的密度公式.

由 2- 秩公式 (推论 2.1(1)) 知, 若 l 是素数, 则 $\mathcal{T}_2(\pm l)$ 和 $\mathcal{T}_2(\pm 2l)$ 当 $l\equiv\pm 3 \pmod 8$ 时是平凡的, 而当 $l\equiv\pm 1 \pmod 8$ 时是非平凡循环群. 假设 $l\equiv\pm 1 \pmod 8$ 是素数. 记 $\mathcal{T}_2(m)$ 的阶是 $t_2(m)$. 我们有如下扩展的 Cohen-Lenstra 猜想:

猜想 4.2 设所有出现的 l 都是素数.

(1) 序列 $\{\mathcal{T}_2(-l)\}_{l\equiv 1 \pmod{16}}$ 关于 (V_3,ω_1) 均匀分布, 序列 $\{\mathcal{T}_2(-2l)\}_{l\equiv 1 \pmod{16}}$ 关于 (V_2,ω_1) 均匀分布.

(2) 序列 $\{\mathcal{T}_2(l)\}_{l\equiv 1 \pmod 8}$、$\{\mathcal{T}_2(2l)\}_{l\equiv 1 \pmod 8}$ 和 $\{\mathcal{T}_2(2l)\}_{l\equiv 7 \pmod 8}$ 都关于 (V_1,ω_0) 均匀分布, 而序列 $\{\mathcal{T}_2(l)\}_{l\equiv 7 \pmod 8}$ 关于 (V_2,ω_0) 均匀分布.

特别地, 对于 $k\geqslant 0$ 且 $e\in\{0,1\}$, 有

$$\lim_{X\to\infty}\frac{\#\{l\leqslant X : l\equiv 1 \pmod{16}, t_2(-l)=2^{k+3}\}}{\#\{l\leqslant X : l\equiv 1 \pmod{16}\}} = \frac{3}{4^{k+1}}, \tag{4.5}$$

$$\lim_{X\to\infty}\frac{\#\{l\leqslant X : l\equiv (-1)^e \pmod 8,\ t_2(l)=2^{k+1+e}\}}{\#\{l\leqslant X : l\equiv (-1)^e \pmod 8\}} = \frac{1}{2^{k+1}}, \tag{4.6}$$

$$\lim_{X\to\infty}\frac{\#\{l\leqslant X: l\equiv(-1)^e \pmod 8,\ t_2(2l)=2^{k+1}\}}{\#\{l\leqslant X: l\equiv(-1)^e \pmod 8\}}=\frac{1}{2^{k+1}}. \tag{4.7}$$

关于此猜想, 我们在文献 [38] 中证明了如下结果, 其中关键点是证明同余式 $t_2(l)\equiv 2t_2(2l)\equiv h_2(-2l) \pmod{16}$ 对于所有 $l\equiv 7 \pmod 8$ 成立 (故它们小于 16 时必相等), 并应用虚二次域的 2- 类群相关结果:

定理 4.2 对于 $k\in\{0,1\}$ 且 $e\in\{0,1\}$, 有

$$\lim_{X\to\infty}\frac{\#\{l\leqslant X: l\equiv(-1)^e \pmod 8,\ t_2(l)=2^{k+1+e}\}}{\#\{l\leqslant X: l\equiv(-1)^e \pmod 8\}}=\frac{1}{2^{k+1}}, \tag{4.8}$$

$$\lim_{X\to\infty}\frac{\#\{l\leqslant X: l\equiv(-1)^e \pmod 8,\ t_2(2l)=2^{k+1}\}}{\#\{l\leqslant X: l\equiv(-1)^e \pmod 8\}}=\frac{1}{2^{k+1}}. \tag{4.9}$$

命题 4.1 (1) 猜想 1.2 等价于等式 (4.6);

(2) 猜想 1.1 的等式 (1.2) 在 $k=0$ 和 $k=1$ 的情形成立.

证明 (1) 设 $a_l+b_l\sqrt{l}$ 是 $\mathbb{Q}(\sqrt{l})$ 的基本单位, 则命题 2.1 说明 $\nu_2(t_2(l))=\nu_2(a_l)-1$ 对于素数 $l\equiv\pm1\pmod 8$ 成立. 故猜想 1.2 等价于 (4.6).

(2) 对于 $l\equiv 9 \pmod{16}$, 文献 [38] 说明 $t_2(l)=2$ 当且仅当 $h_2(-l)=4$, $t_2(l)=4$ 当且仅当 $h_2(-l)\geqslant 16$, 这样, 等式 (1.2) 与它的等价形式 (1.4) 在 $k=0$ 和 $k=1$ 的情形实际上等价于等式 (1.1) 在 $k=0$ 和 $k=1$ 的情形, 我们在定理 3.4 对此已经证明. □

注 4.3 事实上, 关于 $\mathcal{T}_2$- 群的分布, 我们也可以给出更多的扩展猜想. 例如, 我们还猜测序列 $\{\mathcal{T}_2(l)\}_{l\equiv 9 \pmod{16}}$ 和 $\{\mathcal{T}_2(l)\}_{l\equiv 1 \pmod{16}}$ 均关于 (V_1,ω_0) 均匀分布. 上面的命题 (2) 即是 $l\equiv 9 \pmod{16}$ 情形时的理论证据. 我们的数值结果也支持这些猜想.

5 数值依据

本节给出数值证据来支持我们的猜想. 注意到本文新给出的猜想包括关于 $\mathcal{T}_p$- 群的猜想 4.1 和 4.2 以及关于类群的猜想 3.2 和 3.3.

5.1 Pitoun-Varescon 算法

我们应用定理 2.3 来计算二次域的 $\mathcal{T}_p$- 群. 这里计算使用 PARI/GP (参见文献 [39]). 算法如下.

算法 1 Pitoun-Varescon 算法

1: 固定素数 p, 输入无平方因子整数 d, 使用 PARI/GP 里的函数库里的函数 **bnfinit** 生成域 $K=\mathbb{Q}(\sqrt{d})$.
2: **for** $n=3$ to N **do**
3: 使用 PARI/GP 里的函数库里的函数 **bnrinit** 计算 $\mathcal{A}_{p^n}(K)$ 和 $\mathcal{A}_{p^{n+1}}(K)$, K 关于模 p^n 和 p^{n+1} 的射影类群的 p- 部分.
4: **if** 存在 $a_1,\ldots,a_{r_2(K)+1},b_1,\ldots,b_w$ 使得 $\mathcal{A}_{p^n}(K)$ 和 $\mathcal{A}_{p^{n+1}}(K)$ 满足定理 2.3 中的条件 **then**
5: 输出 $\mathcal{T}_p(K)=\prod\mathbb{Z}/b_i\mathbb{Z}$
6: $n=n+1$
7: **end if**
8: **end for**

5.2 实二次域情形

在表 1–4 中, $p=5$ 或 $p=7$, f 是 $\mathcal{M}_{\mathbb{Z}_p}$ 上的 L^1- 函数, B 是界, 而表中间的值是 $\frac{\sum_D f(\mathcal{T}_p(D))}{\sum_D 1}$, 其中 $D<B$. 如果 $f=1_G$, 则这个值是区间 $[1,B]$ 内所有满足条件 $\mathcal{T}_p(D)\cong G$ 的判别式的密度. 加权均值 $M(f,\mathcal{M}_{\mathbb{Z}_p},\omega_0)$ 由命题 3.1 和 3.2 给出.

5.3 虚二次域情形

在表 5–8 中, $p=5$ 或 $p=7$, f 是 $\mathcal{M}_{\mathbb{Z}_p}$ 上的 L^1- 函数, B 是界, 而表中间的值是 $\frac{\sum_D f(\mathcal{T}_p(D))}{\sum_D 1}$, 其中 $|D|<B$. 如果 $f=1_G$, 则这个值是区间 $[-B,-1]$ 内所有满足条件 $\mathcal{T}_p(D)\cong G$ 的判别式的密度. 加权均值 $M(f,\mathcal{M}_{\mathbb{Z}_p},\omega_1)$ 由命题 3.1 和 3.2 给出.

表 1　实二次域的 $\mathcal{T}_5$ 群同构于 G 的情形

B	G				
	$\mathbb{Z}/5\mathbb{Z}$	$\mathbb{Z}/25\mathbb{Z}$	$(\mathbb{Z}/5\mathbb{Z})^2$	$\mathbb{Z}/5\mathbb{Z}\times\mathbb{Z}/25\mathbb{Z}$	$(\mathbb{Z}/5\mathbb{Z})^3$
1×10^7	0.1876	0.03694	1.375E−3	3.277E−4	0
2×10^7	0.1880	0.03712	1.396E−3	3.463E−4	1.645E−7
3×10^7	0.1880	0.03727	1.416E−3	3.439E−4	2.193E−7
4×10^7	0.1880	0.03739	1.438E−3	3.447E−4	3.290E−7
5×10^7	0.1882	0.03740	1.453E−3	3.430E−4	2.632E−7
$M(f,\mathcal{M}_{\mathbb{Z}_5},\omega_0)$	0.1901	0.03802	1.584E−3	3.802E−4	5.110E−7

表 2　实二次域的 $\mathcal{T}_5$ 群, f 不是特征函数的情形

B	f				
	$1_{\mathcal{M}_1}$	$1_{\mathcal{M}_2}$	$1_{\mathcal{M}_3}$	$5^{\mathrm{rk}_5(G)}$	$5^{2\mathrm{rk}_5(G)}$
1×10^7	0.2336	1.791E−3	0	1.977	7.723
2×10^7	0.2343	1.832E−3	1.645E−7	1.981	7.768
3×10^7	0.2345	1.847E−3	2.193E−7	1.982	7.785
4×10^7	0.2347	1.871E−3	3.290E−7	1.984	7.806
5×10^7	0.2348	1.883E−3	2.632E−7	1.985	7.815
$M(f,\mathcal{M}_{\mathbb{Z}_5},\omega_0)$	0.2376	2.063E−3	6.707E−7	2	8

表 3　实二次域的 $\mathcal{T}_7$ 群同构于 G 的情形

B	G			
	$\mathbb{Z}/7\mathbb{Z}$	$\mathbb{Z}/49\mathbb{Z}$	$(\mathbb{Z}/7\mathbb{Z})^2$	$(\mathbb{Z}/7\mathbb{Z})^3$
1×10^7	0.1377	0.01950	3.622E−4	0
2×10^7	0.1382	0.01956	3.622E−4	0
3×10^7	0.1383	0.01963	3.713E−4	0
4×10^7	0.1385	0.01966	3.764E−4	0
5×10^7	0.1385	0.01968	3.833E−4	5.483E−8
$M(1_G,\mathcal{M}_{\mathbb{Z}_7},\omega_0)$	0.1395	0.01992	4.151E−4	2.477E−8

表 4 实二次域的 $\mathcal{T}_7$ 群, f 不是特征函数的情形

B	f				
	$1_{\mathcal{M}_1}$	$1_{\mathcal{M}_2}$	$1_{\mathcal{M}_3}$	$7^{\mathrm{rk}_7(G)}$	$7^{2\mathrm{rk}_7(G)}$
1×10^7	0.1604	4.257E−4	0	1.983	9.722
2×10^7	0.1610	4.293E−4	0	1.987	9.760
3×10^7	0.1612	4.373E−4	0	1.988	9.786
4×10^7	0.1613	4.429E−4	0	1.989	9.804
5×10^7	0.1614	4.519E−4	0	1.990	9.833
$M(f,\mathcal{M}_{\mathbb{Z}_7},\omega_0)$	0.1627	4.953E−4	2.959E−8	2	10

表 5 虚二次域的 $\mathcal{T}_5$ 群同构于 G 的情形

B	G				
	$\mathbb{Z}/5\mathbb{Z}$	$\mathbb{Z}/25\mathbb{Z}$	$(\mathbb{Z}/5\mathbb{Z})^2$	$\mathbb{Z}/5\mathbb{Z}\times\mathbb{Z}/25\mathbb{Z}$	$(\mathbb{Z}/5\mathbb{Z})^3$
1×10^7	0.04558	1.767E−3	6.185E−5	6.580E−7	0
2×10^7	0.04584	1.789E−3	6.004E−5	1.645E−6	0
3×10^7	0.04604	1.801E−3	6.152E−5	2.084E−6	0
4×10^7	0.04613	1.809E−3	6.424E−5	2.385E−6	0
5×10^7	0.04618	1.915E−3	6.659E−5	2.237E−6	0
$M(1_G,\mathcal{M}_{\mathbb{Z}_5},\omega_1)$	0.04752	1.901E−3	7.920E−5	3.802E−6	5.110E−9

表 6 虚二次域的 $\mathcal{T}_5$ 群, f 不是特征函数的情形

B	f				
	$1_{\mathcal{M}_1}$	$1_{\mathcal{M}_2}$	$1_{\mathcal{M}_3}$	$5^{\mathrm{rk}_5(G)}$	$5^{2\mathrm{rk}_5(G)}$
1×10^7	0.04741	6.251E−5	0	1.191	2.177
2×10^7	0.04769	6.168E−5	0	1.192	2.183
3×10^7	0.04790	6.360E−5	0	1.193	2.189
4×10^7	0.04801	6.662E−5	0	1.194	2.194
5×10^7	0.04807	6.882E−5	0	1.194	2.197
$M(f,\mathcal{M}_{\mathbb{Z}_5},\omega_1)$	0.04950	8.317E−5	5.374E−9	1.2	2.24

表 7 虚二次域的 $\mathcal{T}_7$ 群同构于 G 的情形

B	G			
	$\mathbb{Z}/7\mathbb{Z}$	$\mathbb{Z}/49\mathbb{Z}$	$(\mathbb{Z}/7\mathbb{Z})^2$	$(\mathbb{Z}/7\mathbb{Z})^3$
1×10^7	0.02287	0.00043	3.619E−6	0
2×10^7	0.02297	0.00045	5.263E−6	0
3×10^7	0.02302	0.00045	5.593E−6	0
4×10^7	0.02307	0.00045	6.827E−6	0
5×10^7	0.02307	0.00045	7.435E−6	0
$M(1_G,\mathcal{M}_{\mathbb{Z}_7},\omega_1)$	0.02324	0.00047	9.883E−6	8.425E−11

表 8　虚二次域的 $\mathcal{T}_7$ 群, f 不是特征函数的情形

B	f				
	$1_{\mathcal{M}_1}$	$1_{\mathcal{M}_2}$	$1_{\mathcal{M}_3}$	$7^{\mathrm{rk}_7(G)}$	$7^{2\mathrm{rk}_7(G)}$
1×10^7	0.02331	3.619E−6	0	1.140	2.128
2×10^7	0.02342	5.264E−6	0	1.141	2.137
3×10^7	0.02348	5.702E−6	0	1.141	2.141
4×10^7	0.02352	6.909E−6	0	1.141	2.146
5×10^7	0.02353	7.567E−6	0	1.142	2.148
$M(f,\mathcal{M}_{\mathbb{Z}_7},\omega_1)$	0.02373	1.012E−5	8.629E−11	1.143	2.163

5.4　关于 $\mathcal{T}_2$- 群的扩展猜想

在表 9–14 中, (i) $m=-l$ 或 $m=-2l$, $l\equiv1\ (\mathrm{mod}\ 16)$ 是素数或 (ii) $m=l$ 或 $m=2l$, $l\equiv\pm1\ (\mathrm{mod}\ 8)$ 是素数. 对于函数 f 和界 B, 表中间值是 $\frac{\sum_{l<B}f(\mathcal{T}_2(m))}{\sum_{l<B}1}$. 由命题 3.2, 我们有如下引理.

引理 5.1　设 $V_j=\{\mathbb{Z}/2^k\mathbb{Z}:k\geqslant j\}$, $\boldsymbol{k}$ 是函数 $V_j\to\mathbb{Z}$, $\boldsymbol{k}(G)=\log_2(|G|)$.

(1) 若 $k\geqslant0$ 且 $j\geqslant1$, 则

$$M(1_{\mathbb{Z}/2^{k+j}\mathbb{Z}},V_j,\omega_0)=\frac{1}{2^{k+1}}.$$

(2)

$$M(2^{\boldsymbol{k}},V_3,\omega_1)=12,\quad M(\boldsymbol{k},V_3,\omega_1)=\frac{10}{3},\quad M((-2)^{\boldsymbol{k}},V_3,\omega_1)=-4,$$
$$M(2^{\boldsymbol{k}},V_2,\omega_1)=6,\quad M(\boldsymbol{k},V_2,\omega_1)=\frac{7}{3},\quad M((-2)^{\boldsymbol{k}},V_2,\omega_1)=2,$$
$$M\left(\frac{2^{\boldsymbol{k}}}{\boldsymbol{k}^2},V_1,\omega_0\right)=\frac{\pi^2}{6},\quad M(\boldsymbol{k},V_1,\omega_0)=2,\quad M\left(\frac{(-2)^{\boldsymbol{k}}}{\boldsymbol{k}^2},V_1,\omega_0\right)=-\frac{\pi^2}{12},$$
$$M\left(\frac{2^{\boldsymbol{k}}}{\boldsymbol{k}^2},V_2,\omega_0\right)=\frac{\pi^2}{3}-2,\quad M(\boldsymbol{k},V_2,\omega_0)=3,\quad M\left(\frac{(-2)^{\boldsymbol{k}}}{\boldsymbol{k}^2},V_2,\omega_0\right)=2-\frac{\pi^2}{6}.$$

5.5　关于 2- 类群的扩展猜想

表 15 和 16 分别用来支持猜想 3.2 和 3.3. 由于特征函数情形已经被考虑过, 此处只考虑非特征函数. 这里 $m=-l$ 或 $m=-2l$, l 是 $\pm1\ (\mathrm{mod}\ 8)$ 或者 $1\ (\mathrm{mod}\ 16)$ 中的素数. 对于函数 f 和界 B, 表中间值是 $\frac{\sum_{l<B}f(\mathrm{Cl}_2(m))}{\sum_{l<B}1}$.

表 9　$\mathcal{T}_2(-l)$, $l\equiv1\ (\mathrm{mod}\ 16)$ 且为素数

B	f							
	$1_{\mathbb{Z}/8\mathbb{Z}}$	$1_{\mathbb{Z}/16\mathbb{Z}}$	$1_{\mathbb{Z}/32\mathbb{Z}}$	$1_{\mathbb{Z}/64\mathbb{Z}}$	$1_{\mathbb{Z}/128\mathbb{Z}}$	$2^{\boldsymbol{k}}$	$\boldsymbol{k}$	$(-2)^{\boldsymbol{k}}$
1×10^7	0.7508	0.1867	0.04704	0.01172	2.905E−3	11.90	3.332	−3.992
2×10^7	0.7501	0.1872	0.04708	0.01170	3.062E−3	11.96	3.333	−4.015
3×10^7	0.7501	0.1878	0.04658	0.01169	2.977E−3	11.95	3.333	−3.978
4×10^7	0.7498	0.1881	0.04666	0.01166	2.910E−3	11.96	3.333	−3.979
5×10^7	0.7496	0.1880	0.04694	0.01160	2.934E−3	11.97	3.333	−3.986
$M(f,V_3,\omega_1)$	0.7500	0.1875	0.04688	0.01172	2.930E−3	12.00	3.333	−4.000

表 10 $\mathcal{T}_2(-2l)$, $l\equiv 1\ (\mathrm{mod}\ 16)$ 且为素数

B	f							
	$1_{\mathbb{Z}/4\mathbb{Z}}$	$1_{\mathbb{Z}/8\mathbb{Z}}$	$1_{\mathbb{Z}/16\mathbb{Z}}$	$1_{\mathbb{Z}/32\mathbb{Z}}$	$1_{\mathbb{Z}/64\mathbb{Z}}$	2^k	k	$(-2)^k$
1×10^7	0.7508	0.1876	0.04611	0.01144	3.134E−3	5.977	2.331	2.049
2×10^7	0.7501	0.1886	0.04604	0.01142	3.075E−3	5.969	2.331	2.008
3×10^7	0.7501	0.1885	0.04611	0.01140	3.029E−3	5.974	2.332	2.011
4×10^7	0.7498	0.1885	0.04633	0.01153	3.032E−3	5.981	2.333	2.008
5×10^7	0.7496	0.1883	0.04655	0.01157	3.051E−3	5.998	2.333	2.016
$M(f,V_2,\omega_1)$	0.7500	0.1875	0.04688	0.01172	2.930E−3	6.000	2.333	2.000

表 11 $\mathcal{T}_2(l)$, $l\equiv 1\ (\mathrm{mod}\ 8)$ 且为素数

B	f								
	$1_{\mathbb{Z}/2\mathbb{Z}}$	$1_{\mathbb{Z}/4\mathbb{Z}}$	$1_{\mathbb{Z}/8\mathbb{Z}}$	$1_{\mathbb{Z}/16\mathbb{Z}}$	$1_{\mathbb{Z}/32\mathbb{Z}}$	$1_{\mathbb{Z}/64\mathbb{Z}}$	$\frac{2^k}{k^2}$	k	$\frac{(-2)^k}{k^2}$
1×10^7	0.5002	0.2499	0.1245	0.06236	0.03169	0.01553	1.609	2.001	−0.8054
2×10^7	0.5000	0.2499	0.1245	0.06255	0.03163	0.01567	1.634	2.003	−0.7914
3×10^7	0.5005	0.2496	0.1246	0.06278	0.03115	0.01560	1.835	2.000	−0.5900
4×10^7	0.5003	0.2496	0.1247	0.06278	0.03115	0.01564	1.780	2.001	−0.6481
5×10^7	0.5001	0.2497	0.1247	0.06281	0.03116	0.01567	1.746	2.001	−0.6812
$M(f,V_1,\omega_0)$	0.5000	0.2500	0.1250	0.06250	0.03125	0.01563	1.645	2.000	−0.8225

表 12 $\mathcal{T}_2(l)$, $l\equiv 7\ (\mathrm{mod}\ 8)$ 且为素数

B	f								
	$1_{\mathbb{Z}/4\mathbb{Z}}$	$1_{\mathbb{Z}/8\mathbb{Z}}$	$1_{\mathbb{Z}/16\mathbb{Z}}$	$1_{\mathbb{Z}/32\mathbb{Z}}$	$1_{\mathbb{Z}/64\mathbb{Z}}$	$1_{\mathbb{Z}/128\mathbb{Z}}$	$\frac{2^k}{k^2}$	k	$\frac{(-2)^k}{k^2}$
1×10^7	0.5000	0.2484	0.1260	0.06361	0.03103	0.01518	1.179	3.001	0.3596
2×10^7	0.5000	0.2494	0.1255	0.06265	0.03123	0.01534	1.209	3.001	0.3827
3×10^7	0.4998	0.2497	0.1252	0.06278	0.03109	0.01557	1.198	3.002	0.3749
4×10^7	0.4999	0.2497	0.1254	0.06246	0.03112	0.01570	1.196	3.001	0.3663
5×10^7	0.5001	0.2497	0.1254	0.06237	0.03116	0.01570	1.214	3.000	0.3435
$M(f,V_2,\omega_0)$	0.5000	0.2.500	0.1250	0.06250	0.03125	0.01563	1.290	3.000	0.3551

表 13 $\mathcal{T}_2(2l)$, $l\equiv 1\ (\mathrm{mod}\ 8)$ 且为素数

B	f								
	$1_{\mathbb{Z}/2\mathbb{Z}}$	$1_{\mathbb{Z}/4\mathbb{Z}}$	$1_{\mathbb{Z}/8\mathbb{Z}}$	$1_{\mathbb{Z}/16\mathbb{Z}}$	$1_{\mathbb{Z}/32\mathbb{Z}}$	$1_{\mathbb{Z}/64\mathbb{Z}}$	$\frac{2^k}{k^2}$	k	$\frac{(-2)^k}{k^2}$
1×10^7	0.5006	0.2515	0.1237	0.06214	0.03100	0.01564	1.601	1.996	−0.8120
2×10^7	0.5004	0.2511	0.1239	0.06219	0.03105	0.01576	1.597	1.998	−0.8238
3×10^7	0.5001	0.2506	0.1245	0.06256	0.03093	0.01572	1.595	1.999	−0.8237
4×10^7	0.5001	0.2505	0.1249	0.06233	0.03090	0.01564	1.619	1.999	−0.8513
5×10^7	0.5000	0.2503	0.1252	0.06236	0.03083	0.01572	1.615	1.999	−0.8506
$M(f,V_1,\omega_0)$	0.5000	0.2500	0.1250	0.06250	0.03125	0.01563	1.645	2.000	−0.8225

表 14　$\mathcal{T}_2(2l)$, $l\equiv 7\pmod 8$ 且为素数

B	f								
	$1_{\mathbb{Z}/2\mathbb{Z}}$	$1_{\mathbb{Z}/4\mathbb{Z}}$	$1_{\mathbb{Z}/8\mathbb{Z}}$	$1_{\mathbb{Z}/16\mathbb{Z}}$	$1_{\mathbb{Z}/32\mathbb{Z}}$	$1_{\mathbb{Z}/64\mathbb{Z}}$	$\frac{2^k}{k^2}$	k	$\frac{(-2)^k}{k^2}$
1×10^7	0.5000	0.2484	0.1253	0.06378	0.03129	0.01565	1.600	2.004	−0.8315
2×10^7	0.5000	0.2.494	0.1253	0.06258	0.03137	0.01565	1.602	2.001	−0.8189
3×10^7	0.4998	0.2497	0.1254	0.06258	0.03116	0.01575	1.598	2.001	−0.8198
4×10^7	0.4999	0.2497	0.1252	0.06267	0.03129	0.01569	1.598	2.001	−0.8251
5×10^7	0.5001	0.2497	0.1250	0.06268	0.03126	0.01573	1.597	2.001	−0.8265
$M(f,V_1,\omega_0)$	0.5000	0.2500	0.1250	0.06250	0.03125	0.01.563	1.645	2.000	−0.8225

表 15　$\mathbb{Q}(\sqrt{-l})$ 和 $\mathbb{Q}(\sqrt{-2l})$ 的 2- 类群, $l\equiv\pm 1\pmod 8$ 为素数

B	f								
	$\frac{2^k}{k^2}$			k			$\frac{(-2)^k}{k^2}$		
	I	II	III	I	II	III	I	II	III
1×10^7	1.118	1.123	1.131	2.989	2.990	3.000	0.3550	0.3544	0.3569
2×10^7	1.127	1.128	1.133	2.994	2.991	2.999	0.1245	0.3524	0.3574
3×10^7	1.131	1.132	1.136	2.994	2.992	2.999	0.3542	0.3544	0.3579
4×10^7	1.133	1.136	1.140	2.985	2.994	2.998	0.3528	0.3566	0.3575
5×10^7	1.134	1.139	1.141	2.996	2.996	2.998	0.3534	0.3562	0.3576
$M(f,V_2,\omega_0)$	$\pi^2/3-2$			3.000			$2-\pi^2/6$		

注: I. $\mathbb{Q}(\sqrt{-l})$, $l\equiv 1\pmod 8$; II. $\mathbb{Q}(\sqrt{-2l})$, $l\equiv 1\pmod 8$; III. $\mathbb{Q}(\sqrt{-2l})$, $l\equiv 7\pmod 8$

表 16　$\mathbb{Q}(\sqrt{-l})$ 和 $\mathbb{Q}(\sqrt{-2l})$ 的 2- 类群, 其中 $l\equiv 9\pmod{16}$ 为素数

B	f					
	$\frac{2^k}{k^2}$		k		$\frac{(-2)^k}{k^2}$	
	$\mathrm{Cl}_2(-l)$	$\mathrm{Cl}_2(-2l)$	$\mathrm{Cl}_2(-l)$	$\mathrm{Cl}_2(-2l)$	$\mathrm{Cl}_2(-l)$	$\mathrm{Cl}_2(-2l)$
1×10^7	1.116	1.125	2.991	2.996	0.3502	0.3540
2×10^7	1.124	1.130	2.993	2.995	0.3490	0.3511
3×10^7	1.130	1.133	2.993	2.995	0.3520	0.3520
4×10^7	1.133	1.138	2.995	2.997	0.3506	0.3540
5×10^7	1.135	1.140	2.995	2.998	0.3530	0.3542
$M(f,V_2,\omega_0)$	$\pi^2/3-2$		3.000		$2-\pi^2/6$	

参考文献

1 Gras G. Groupe de Galois de la p-extension abélienne p-ramifiée maximale d'un corps de nombres. J Reine Angew Math, 1982, 333: 86–132

2 Nguyen-Quang-Do T. Sur la $\mathbb{Z}_p$-torsion de certains modules galoisiens. Ann Inst Fourier (Grenoble), 1986, 36: 27–46

3 Maire C, Rougnant M. A note on p-rational fields and the abc-conjecture. Proc Amer Math Soc, 2020, 148: 3263–3271

4 Pitoun F, Varescon F. Computing the torsion of the p-ramified module of a number field. Math Comp, 2015, 84: 371–383

5 Shanks D C, Sime P J, Washington L C. Zeros of 2-adic L-functions and congruences for class numbers and fundamental

units. Math Comp, 1999, 68: 1243–1255
6 Coates J. p-adic L-functions and Iwasawa's theory. In: Algebraic Number Fields: L-Functions and Galois Properties. London: Academic Press, 1977, 269–353
7 Gras G. Class Field Theory: From Theory to Practice. Translated from the French manuscript by Henri Cohen. Springer Monographs in Mathematics. Berlin: Springer-Verlag, 2003
8 Gras G. The p-adic Kummer-Leopoldt constant: Normalized p-adic regulator. Int J Number Theory, 2018, 14: 329–337
9 Washington L C. Introduction to Cyclotomic Fields. Graduate Texts in Mathematics, vol. 83. New York: Springer, 1997
10 Zhang Z, Yue Q. Fundamental units of real quadratic fields of odd class number. J Number Theory, 2014, 137: 122–129
11 Cohen H, Lenstra Jr H W. Heuristics on class groups of number fields. In: Number Theory. Lecture Notes in Mathematics, vol. 1068. Berlin: Springer, 1984, 33–62
12 Bhargava M, Kane D M, Lenstra Jr H W, et al. Modeling the distribution of ranks, Selmer groups, and Shafarevich-Tate groups of elliptic curves. Camb J Math, 2015, 3: 275–321
13 Park J, Poonen B, Voight J, et al. A heuristic for boundedness of ranks of elliptic curves. J Eur Math Soc (JEMS), 2019, 21: 2859–2903
14 Friedman E, Washington L C. On the distribution of divisor class groups of curves over a finite field. In: Théorie des Nombres. Berlin: de Gruyter, 1989, 227–239
15 Bartel A, Lenstra Jr H W. On class groups of random number fields. Proc Lond Math Soc (3), 2020, 121: 927–953
16 Delaunay C. Heuristics on Tate-Shafarevitch groups of elliptic curves defined over $\mathbb{Q}$. Experiment Math, 2001, 10: 191–196
17 Gerth III F. The 4-class ranks of quadratic extensions of certain imaginary quadratic fields. Illinois J Math, 1989, 33: 132–142
18 Malle G. Cohen-Lenstra heuristic and roots of unity. J Number Theory, 2008, 128: 2823–2835
19 Gerth III F. On p-class groups of cyclic extensions of prime degree p of number fields. Acta Arith, 1991, 60: 85–92
20 Cohen H, Martinet J. Class groups of number fields: Numerical heuristics. Math Comp, 1987, 48: 123–137
21 Cohen H, Martinet J. Étude heuristique des groupes de classes des corps de nombres. J Reine Angew Math, 1990, 404: 39–76
22 Cohen H, Martinet J. Heuristics on class groups: Some good primes are not too good. Math Comp, 1994, 63: 329–334
23 Fouvry E, Klüners J. On the 4-rank of class groups of quadratic number fields. Invent Math, 2007, 167: 455–513
24 Smith A. 2^∞-Selmer groups, 2^∞-class groups, and Goldfeld's conjecture. arXiv:1702.02325, 2017
25 Wood M M. Asymptotics for number fields and class groups. In: Directions in Number Theory. Association for Women in Mathematics Series, vol. 3. Cham: Springer, 2016, 291–339
26 Koymans P, Pagano C. On the distribution of $\mathrm{Cl}(K)[l^\infty]$ for degree l cyclic fields. arXiv:1812.06884, 2018
27 Koymans P. The 16-rank of $\mathbb{Q}(\sqrt{-p})$. Algebra Number Theory, 2020, 14: 37–65
28 Koymans P, Milovic D. On the 16-rank of class groups of $\mathbb{Q}(\sqrt{-2p})$ for primes $p \equiv 1$ mod 4. Int Math Res Not IMRN, 2019, 2019: 7406–7427
29 Milovic D. On the 16-rank of class groups of $\mathbb{Q}(\sqrt{-8p})$ for $p \equiv -1$ mod 4. Geom Funct Anal, 2017, 27: 973–1016
30 Stevenhagen P. Class groups and governing fields. PhD Thesis. Berkeley: University of California, 1988
31 Stevenhagen P. Divisibility by 2-powers of certain quadratic class numbers. J Number Theory, 1993, 43: 1–19
32 Hasse H. Über die Klassenzahl des Körpers $P(\sqrt{-2p})$ mit einer Primzahl $p \neq 2$. J Number Theory, 1969, 1: 231–234
33 Leonard P A, Williams K S. On the divisibility of the class numbers of $\mathbb{Q}(\sqrt{-p})$ and $\mathbb{Q}(\sqrt{-2p})$ by 16. Canad Math Bull, 1982, 25: 200–206
34 Li J, Xu Y. On class numbers of pure quartic fields. Ramanujan J, 2021, 56: 235–248
35 Jordan B W, Klagsbrun Z, Poonen B, et al. Statistics of K-groups modulo p for the ring of integers of a varying quadratic number field. Tunisian J Math, 2020, 2: 287–307
36 Gerth III F. The 4-class ranks of quadratic fields. Invent Math, 1984, 77: 489–515
37 Yue Q, Yu J. The densities of 4-ranks of tame kernels for quadratic fields. J Reine Angew Math, 2004, 567: 151–173
38 Li J, Ouyang Y, Xu Y. On abelian 2-ramification torsion modules of quadratic fields. arXiv:2009.13262, 2020
39 The PARI Group, Univ. Bordeaux, PARI/GP version 2.7.5. http://pari.math.u-bordeaux.fr/., 2015

Abelian p-ramification groups and new Cohen-Lenstra heuristics

Jianing Li, Yi Ouyang & Yue Xu

Abstract In this paper, we first review the $\mathcal{T}_p$-groups in the abelian p-ramification theory of general number fields. We also review a general setting of the Cohen-Lenstra heuristic. Then we propose various new Cohen-Lenstra heuristics for distributions of $\mathcal{T}_p$-groups of quadratic fields, which in particular explains the speculation of Shanks et al. (1999) on the distributions of zeros of 2-adic L-functions and also reveals the distribution of fundamental units in certain real quadratic fields. Theoretical and numerical evidences of our conjectures are also presented.

Keywords **Cohen-Lenstra heuristic, quadratic field, Abelian p-ramification group, class group, fundamental unit**

MSC(2020) **11R45, 11R11, 11R37**

doi: 10.1360/SSM-2020-0294