中国科学 A辑: 数学 2009 年 第 39 卷 第 2 期: 129～138
www.scichina.com math.scichina.com
《中国科学》杂志社 SCIENCE IN CHINA PRESS

四次循环域类数模 2 的幂的同余公式

马连荣 *, 李伟, 张贤科

清华大学数学科学系, 北京 100084

* E-mail: lrma@math.tsinghua.edu.cn

收稿日期: 2007-11-20; 接受日期: 2008-10-22
国家自然科学基金 (批准号: 10771111) 资助项目

摘要 设 $K=k(\sqrt{\theta})$ 是实四次循环域, k 是其二次子域, $\tilde{K}=k(\sqrt{-\theta})$ 是相应的虚四次循环域. 把 K, k 和 $\tilde{K}$ 的类数分别记为 h_K, h_k 和 $h_{\tilde{K}}$, 本文通过研究 p-adic L-函数, 得到了相对类数 $h^-=h_K/h_k$ 和 $\tilde{h}^-=h_{\tilde{K}}/h_k$ 的模 2 的幂的同余公式.

关键词 类数 正规子 p-adic L- 函数 导子

MSC(2000) 主题分类 11M9, 11R29

1 引言

Ankeny 等在文献 [1] 中得到二次数域 k 的类数 $h(k)$ 的许多同余公式, 其中最著名的是: 若 k 的导子为素数 $p\equiv 1 \pmod 4$, 记 $\varepsilon=(t+u\sqrt{p})/2$ 为 k 的基本单位, 则

$$h(k)\ u/t \equiv B_{(p-1)/2} \pmod p,$$

其中 $B_{(p-1)/2}$ 是 Bernoulli 数. 陆洪文在文献 [2] 中得到二次域的一系列同余公式. 冯克勤在文献 [3] 中成功地将此类同余式推广到了三次循环域. 张贤科在文献 [4,5] 中得到了一般的三次和四次循环域的一系列类数同余公式. 在文献 [6] 中刘通得到了六次循环域的同类公式.

而在模 2 的幂方面, 张贤科在文献 [7] 中给出了一般实二次域 $\mathbb{Q}(\sqrt{m})$ 与相应虚二次域 $\mathbb{Q}(\sqrt{-m})$ 的类数之间的模 8 的一系列同余公式. 本文研究一般实四次循环域, 得到其理想类数的模 2 的幂的一系列同余公式.

以下设 K 是实四次循环域, k 是其二次子域. 于是 $K=k(\sqrt{\theta})$ (其中 $\theta\in k$). 记 $\tilde{K}=k(\sqrt{-\theta})$ 是相应的虚四次循环域. 分别记 K, k 的导子为 F, f; $K, \tilde{K}, k$ 的类数为 h_K, $h_{\tilde{K}}$, h_k. 记 $h_K/h_k=h^-$, $h_{\tilde{K}}/h_k=\tilde{h}^-$ 称为 K 和 $\tilde{K}$ 的相对类数. 由文献 [8] 知, 存在 K/k 的相对基本单位 E, 满足

$$N=N_{K/k}(E)=\pm 1,\qquad Q=(U_K:\langle\varepsilon, E, E^{\sigma}\rangle)=1 \text{ 或 } 2,$$

这里 U_K 表示 K 的单位群, ε 为 k 的基本单位, σ 是 $\mathrm{Gal}(K/\mathbb{Q})$ 的生成元. 本文得到如下各定理.

定理 1.1 设 $16|F, F\neq 16$. 则 $f=8u$, u 的素因子 $p\equiv 1 \pmod 4$, $\mathrm{tr}_{K/k}(E)=2a+2b\sqrt{2u}(a,b\in\mathbb{Z})$, 四次循环域 K 和 $\tilde{K}$ 的相对类数满足如下各公式:

(I.1) $b\ h^-\equiv 0 \pmod{4Q}$ ($N=1$ 时);

(I.2) $(1-a^2)\ h^-\equiv 2Q\ \tilde{h}^- \pmod{8Q}$ ($N=1$ 时);

(I.3) $h^-\equiv 0 \pmod{4Q}$ ($N=-1$ 时);

(I.4) $\tilde{h}^-\equiv 0 \pmod 4$ ($N=-1$ 时).

定理 1.2 设 $8\parallel F$, $f\equiv 5 \pmod 8$. 记 $F_1=F/8$. 则 $\mathrm{tr}_{K/k}E=(2a+b)+b\sqrt{f}$ $(a,b\in\mathbb{Z})$, 四次循环域 K 和 $\tilde{K}$ 的相对类数满足:

(II.1) $h^-(a^2(1-a^2)+b^2(\frac{f-1}{2}a^2-3))\ \equiv QF_1\ \tilde{h}^- \pmod{4Q}$;

(II.2) $h^-(2ab(1-ab)+b^2(\frac{f-1}{2}-1-3b^2))\ \equiv\ 0 \pmod{4Q}$.

定理 1.3 设 $4\parallel F$, $F\neq 20$, $f\equiv 5 \pmod 8$, 则 $\mathrm{tr}_{K/k}E=(2a+b)+b\sqrt{f}$ $(a,b\in\mathbb{Z})$, 四次循环域 K 和 $\tilde{K}$ 的相对类数满足:

(III.1) $b^2h^-\equiv 0 \pmod Q$;

(III.2) $b^2h^-\equiv Q\tilde{h}^- \pmod{2Q}$.

定理 1.4 设 $2\nmid F$, $v_2(\mathrm{tr}_{K/k}E)\geqslant 1$, 则 $\mathrm{tr}_{K/k}E=(2a+b)+b\sqrt{f}$ $(a,b\in\mathbb{Z})$, 四次循环域 K 和 $\tilde{K}$ 的相对类数满足:

(IV.1) $b^2h^-\equiv 0 \pmod Q$;

(IV.2) $2b^2h^-\equiv QF\tilde{h}^- \pmod{4Q}$.

例 1.5 下面用到的数据取自文献 [5, 9].

在定理 1.1 中, 取 $F=80$, 则 $\mathrm{tr}_{K/k}E=14+10\sqrt{2}$ (即 $a=7$, $b=5$), $N=-1$, $Q=1$, 同余式 (I.3), (I.4) 成为 $h^-\equiv 0 \pmod 4$, $\tilde{h}^-\equiv 0 \pmod 4$.

在定理 1.2 中, 取 $F=40$, 则 $f=5$, $F_1=5$, $\mathrm{tr}_{K/k}E=4+2\sqrt{5}$ (即 $a=1$, $b=2$), $Q=1$, 同余式 (II.1) 成为 $\tilde{h}^-\equiv 0 \pmod 4$.

在定理 1.3 中, 取 $F=52$, 则 $f=13$, $\mathrm{tr}_{K/k}E=3+\sqrt{13}$ (即 $a=1$, $b=1$), $Q=1$, 同余式 (III.2) 成为 $h^-\equiv\tilde{h}^- \pmod 2$.

在定理 1.4 中, 取 $F=85$, 则 $f=17$, $\mathrm{tr}_{K/k}E=76+20\sqrt{17}$ (即 $a=28$, $b=20$), $Q=2$. 同余式 (IV.2) 成为 $\tilde{h}^-\equiv 0 \pmod 4$.

2 四次域的结构

由文献 [10] 知, 四次循环域 K 的导子 F 有如下的形式:

$$F=2^{\beta}p_1\cdots p_r,$$

其中 $\beta=0,2,3,4$, p_i $(i=1,\ldots,r)$ 是不同的奇素数.

当 $16|F$ 时, 将 K 的特征群 $\widehat{K}$ 的生成元 χ 分解为 $\chi=\chi_2\chi_{p_1}\cdots\chi_{p_{r_1}}\chi_{p_{r_1+1}}\cdots\chi_{p_r}$, 其中 χ_2 的导子为 16, χ_{p_i} $(1\leqslant i\leqslant r_1)$ 是模 p_i 的纯四次特征, $\chi_{p_j}(r_1<j\leqslant r)$ 是模 p_j 的二次特征, 则 k 的导子 $f=8p_1\cdots p_{r_1}$. 因为 2-Techmüler ω 的导子为 4, 所以 $\chi_2\neq\omega$. 此时, $k=\mathbb{Q}(\sqrt{2p_1\cdots p_{r_1}})$.

当 $8\parallel F$ 时, 对 χ 做类似的分解, $\chi=\chi_2\chi_{p_1}\cdots\chi_{p_{r_1}}\chi_{p_{r_1+1}}\cdots\chi_{p_r}$, 则 $f=p_1\cdots p_{r_1}$. 同样, 因为 χ_2 的导子为 8, 所以 $\chi_2\neq\omega$. 此时, $k=\mathbb{Q}(\sqrt{f})$.

当 $4 \parallel F$ 时, 对 χ 做分解 $\chi=\chi_2\chi_{p_1}\cdots\chi_{p_{r_1}}\chi_{p_{r_1+1}}\cdots\chi_{p_r}$, 则 $f=p_1\cdots p_{r_1}$, $\chi_2=\omega$, $k=\mathbb{Q}(\sqrt{f})$. 因为 χ_{p_1} 是纯四次特征, 所以 $p_i\equiv 1 \pmod 4$ $(i=1,\dots,r_1)$.

当 $2\nmid F$ 时, 将 χ 分解为 $\chi=\chi_{p_1}\cdots\chi_{p_{r_1}}\chi_{p_{r_1+1}}\cdots\chi_{p_r}$, 则 $f=p_1\cdots p_{r_1}$, $k=\mathbb{Q}(\sqrt{f})$.

为了简化后面的运算, 当 $16\nmid F$ 时, 我们假设 $f\equiv 5 \pmod 8$. 在此假设下, $p_1,\dots,p_{r_1}$ 中有奇数个满足 $p_i\equiv 5 \pmod 8$, 即 2 不是模 p_i 的二次剩余, 从而 $\chi_{p_1}(2)\cdots\chi_{p_{r_1}}(2)=\pm i$.

3 类数同余公式

从所周知 (参见文献 [11, 12]), 对于实 n 次 Abel 数域 K, 其类数 $h(K)$ 满足公式

$$\frac{2^{n-1}h(K)R_p(K)}{\sqrt{d(K)}}=\prod_{\substack{\chi\in X,\\ \chi\neq 1}}\left(1-\frac{\chi(p)}{p}\right)^{-1}L_p(1,\chi),$$

其中 $R_p(K)$ 是 K 的 p-adic 正规子, $X=\widehat{K}$ 是 K 的全部 Dirichlet 特征组成的群, L_p 是 p-adic L-函数, $d(K)$ 是域 K 的判别式. 对于我们的实四次循环域 $K=k(\sqrt{\theta})$, 记 $\widehat{K}=X=\langle\chi\rangle$, 则有

$$\frac{2^3h_KR_p}{\sqrt{d(K)}}=y_1^{-1}y_2^{-1}y_3^{-1}L_p(1,\chi)L_p(1,\chi^2)L_p(1,\chi^3), \tag{3.1}$$

其中 $y_i=1-\chi^i(p)/p$ $(i=1,2,3)$. 对于 K 的二次子域 k 的类数 h_k, 有类数公式

$$\frac{2h_kR_p(k)}{\sqrt{d(k)}}=y_2^{-1}L_p(1,\chi^2). \tag{3.2}$$

用公式 (3.1) 除以公式 (3.2) 得到

$$\frac{4h^-R_p^-}{F}=y_1^{-1}y_3^{-1}L_p(1,\chi)L_p(1,\chi^3), \tag{3.3}$$

其中 $R_p^-=R_p(K)/R_p(k)$, 称之为相对正规子.

对于与 K 相应的虚四次循环域 $\tilde{K}$, 因为 $\tilde{K}$ 是 CM 域, 所以 $\widehat{\tilde{K}}=\langle\tilde{\chi}\rangle$, $\tilde{\chi}=\chi\omega$. 并且

$$\tilde{h}^-=h_{\tilde{K}}/h_k=\tilde{Q}z\prod_{\substack{\eta\in\widehat{\tilde{K}},\\ \eta(-1)=-1}}\left(-\frac{1}{2}B_{1,\eta}\right),$$

其中 $\tilde{Q}$ 是 k 在 $\tilde{K}$ 中的自由单位指数, $\tilde{Q}=1$ 或 2, z 是 $\tilde{K}$ 中单位根的个数. 由文献 [8] 知, $\tilde{Q}=1$, $z=2$ $(\tilde{K}\neq\mathbb{Q}(\zeta_5))$ 或 10 $(\tilde{K}=\mathbb{Q}(\zeta_5))$. 当 $\tilde{K}=\mathbb{Q}(\zeta_5)$ 时, $K=\mathbb{Q}(\zeta_{20}+\zeta_{20}^{-1})$, K 的类数 $h_K=1$, 本文不考虑这种特殊情况, 所以假定 $z=2$. 从而有

$$\tilde{h}^-=\frac{1}{2}B_{1,\tilde{\chi}}B_{1,\tilde{\chi}^3}.$$

下面取 $p=2$, 对 F 分情况进行讨论.

若 F 是 2 的幂次, 则 $F=16$ ($(\mathbb{Z}/8\mathbb{Z})^\times$ 是两个 2 阶群的直积), 此时 $K=\mathbb{Q}(\zeta_{16}+\zeta_{16}^{-1})$, K, k, $\tilde{K}$ 的类数都是 1, 本文不考虑这种情况. 因此, 对于 $p=2$, $\widehat{K}$ 的生成元 χ 都不是二类特征 (即: 导子和阶数都是 p 的幂次的特征). 由文献 [13], 有

$$L_2(1,\chi^i)\equiv L_2(0,\chi^i) \pmod 8,\quad i=1,2,3. \tag{3.4}$$

当 $4|F$ 时, $y_1=y_3=1$, 将公式 (3.4) 代入公式 (3.3), 得到

$$\frac{4h^-R_2^-}{F}\equiv L_2(0,\chi)L_2(0,\chi^3) \pmod 8. \tag{3.5}$$

当 $2\nmid F$ 时, 由于假设 $f\equiv 5\ (\mathrm{mod}\ 8)$, 有 $\chi(2)=\pm i$, $\chi^3(2)=\mp i$, 所以 $y_1^{-1}y_3^{-1}=(1-\frac{i}{2})^{-1}(1+\frac{i}{2})^{-1}=\frac{4}{5}$, 将 (3.4) 式代入 (3.3) 式得到

$$\frac{h^-R_2^-}{F}\equiv 5L_2(0,\chi)L_2(0,\chi^3)\ (\mathrm{mod}\ 8). \tag{3.6}$$

再将等式 (参见文献 [14]) $L_2(0,\chi^i)=-(1-\chi^i\omega^{-1}(2))B_{1,\ \chi^i\omega^{-1}}$ 代入 (3.5) 和 (3.6), 得到

$4|F$ 时,

$$\begin{aligned}\frac{4h^-R_2^-}{F}&\equiv(1-\chi\omega^{-1}(2))(1-\chi^3\omega^{-1}(2))B_{1,\ \chi\omega^{-1}}B_{1,\ \chi^3\omega^{-1}}\\&\equiv 2\ (1-\chi\omega^{-1}(2))(1-\chi^3\omega^{-1}(2))\tilde{h}^-(\mathrm{mod}\ 8).\end{aligned} \tag{3.5.1}$$

$2\nmid F$ 时,

$$\begin{aligned}\frac{h^-R_2^-}{F}&\equiv 5(1-\chi\omega^{-1}(2))(1-\chi^3\omega^{-1}(2))B_{1,\chi\omega^{-1}}B_{1,\chi^3\omega^{-1}}\\&\equiv 2\ (1-\chi\omega^{-1}(2))(1-\chi^3\omega^{-1}(2))\tilde{h}^-(\mathrm{mod}\ 8).\end{aligned} \tag{3.6.1}$$

情形 1 $16|F$. 此时, 因为 $\chi_2\neq\omega$, 所以 $1-\chi\omega^{-1}(2)=1-\chi^3\omega^{-1}(2)=1$, 记 $F=16F_1$, 则公式 (3.5.1) 成为

$16|F$ 时,

$$h^-R_2^-\equiv 8F_1\tilde{h}^-\ (\mathrm{mod}\ 32). \tag{3.7}$$

情形 2 $8\parallel F$. 此时, 由 $\chi_2\neq\omega$, 从而 $1-\chi\omega^{-1}(2)=1-\chi^3\omega^{-1}(2)=1$, 记 $F=8F_1$, 则公式 (3.5.1) 为

$8\|F$ 时,

$$h^-R_2^-\equiv 4F_1\tilde{h}^-\ (\mathrm{mod}\ 16). \tag{3.8}$$

情形 3 $4\parallel F$. 此时, 因为 $\chi_2=\omega$, $f\equiv 5\ (\mathrm{mod}\ 8)$, 所以 $(1-\chi\omega^{-1}(2))(1-\chi^3\omega^{-1}(2))=(1-i)(1+i)=2$, 记 $F=4F_1$, 则公式 (3.5.1) 成为

$4\|F$ 时,

$$h^-R_2^-\equiv 4F_1\tilde{h}^-\ (\mathrm{mod}\ 8). \tag{3.9}$$

情形 4 $2\nmid F$. 此时, $1-\chi\omega^{-1}(2)=1=1-\chi^3\omega^{-1}(2)$, 公式 (3.6.1) 成为

$2\nmid F$ 时,

$$h^-R_2^-\equiv 2F\tilde{h}^-\ (\mathrm{mod}\ 8). \tag{3.10}$$

4 相对正规子

设 $T=\mathrm{tr}_{K/k}(E)$, $N=N_{K/k}(E)=\pm1$, 则 $E=\frac{1}{2}(T\pm\sqrt{T^2-4N})$. 不失一般性, 总假设 $E=\frac{1}{2}(T+\sqrt{T^2-4N})$, $E^\sigma=\frac{1}{2}(T-\sqrt{T^2-4N})$. 由文献 [5] 知, $R_2^-=2(\log_2^2E+\log_2^2E^\sigma)/Q$. 我们先来算出 $\log_2^2E+\log_2^2E^\sigma(\mathrm{mod}\ 32)$ 的同余公式, 再分情况进行分析. 首先假设 $v_2(T)\geqslant 1$, 这里 v_2 是 $\overline{\mathbb{Q}}_2$ 上的标准指数赋值, $v_2(2)=1$. 在后面的讨论中可以看到, 当 $16|F$ 或 $4|F$ 且 $f\equiv 5\ (\mathrm{mod}\ 8)$ 时, 必有 $v_2(T)\geqslant 1$.

记 $A=2E=T+\sqrt{T^2-4N}$, $\bar{A}=2E^\sigma$, 则 $v_2(A)=v_2(\bar{A})=v_2(2)$. 记 $B=NTA/2$, $\bar{B}=NT\bar{A}/2$, 则 $v_2(B)=v_2(\bar{B})=v_2(T)\geqslant 1$. 于是,

$$\log_2E=\frac{1}{2}\log_2(E^2)=\frac{1}{2}\log_2\left(1-\frac{NT}{2}(T+\sqrt{T^2-4NT})\right)$$

$$= \frac{1}{2}\log_2(1-B) \equiv -\frac{1}{2}\left(B+\frac{B^2}{2}+\frac{B^3}{3}+\frac{B^4}{4}\right) \pmod{16},$$

$$\log_2^2 E \equiv \frac{1}{4}\left(B^2+B^3+\frac{11}{12}B^4+\frac{5}{6}B^5+\frac{13}{36}B^6+\frac{1}{6}B^7+\frac{1}{16}B^8\right) \pmod{32}.$$

因为 $B+\bar{B}=\frac{NT}{2}(A+\bar{A})=NT^2$, $B\cdot\bar{B}=\frac{T^2}{4}A\cdot\bar{A}=\frac{T^2}{4}(T^2-T^2+4N)=NT^2$, 记 $Z=NT^2$, 则有

$$B^2+\bar{B}^2=(B+\bar{B})^2-2(B\cdot\bar{B})=Z^2-2Z,$$

$$B^3+\bar{B}^3=(B^2+\bar{B}^2)(B+\bar{B})-B\bar{B}(B+\bar{B})=(Z^2-2Z)Z-Z^2=Z^3-3Z^2,$$

$$B^4+\bar{B}^4=(B^2+\bar{B}^2)^2-2(B\bar{B})^2=Z^4-4Z^3+2Z^2,$$

$$B^5+\bar{B}^5=(B^4+\bar{B}^4)(B+\bar{B})-B\bar{B}(B^3+\bar{B}^3)=Z^5-5Z^4+5Z^3,$$

$$B^6+\bar{B}^6=(B^3+\bar{B}^3)^2-2(B\bar{B})^3=Z^6-6Z^5+9Z^4-2Z^3,$$

$$B^7+\bar{B}^7=(B^6+\bar{B}^6)(B+\bar{B})-B\bar{B}(B^5+\bar{B}^5)=Z^7-7Z^6+14Z^5-7Z^4,$$

$$B^8+\bar{B}^8=(B^4+\bar{B}^4)^2-2(B\bar{B})^4=Z^8-8Z^7+20Z^6-16Z^5+2Z^4,$$

从而有

$$\begin{aligned}\log_2^2 E+\log_2^2 E^\sigma \equiv \frac{1}{4}\Big(&(Z^2-2Z)+(Z^3-3Z^3)+\frac{11}{12}(Z^4-4Z^3+2Z^2)\\&+\frac{5}{6}(Z^5-5Z^4+5Z^3)+\frac{13}{36}(Z^6-6Z^5+9Z^4-2Z^3)\\&+\frac{1}{6}(Z^7-7Z^6+14Z^5-7Z^4)\\&+\frac{1}{16}(Z^8-8Z^7+20Z^6-16Z^5+2Z^4)\Big) \pmod{32}\\ \equiv \frac{1}{4}\Big(&-2Z-\frac{1}{6}Z^2+\frac{7}{9}Z^3+\frac{1}{8}Z^4\Big) \pmod{32}.\end{aligned}$$

下面将根据 F 的不同情形, 计算出 R_2^- 的同余式, 代入类数同余公式 (3.7)–(3.10) 中, 进而得到所要证明的结果.

5 定理证明

5.1 $16|F$ 的情形

引理 5.1 记 $\mathrm{tr}_{K/k}(E)=T=\alpha+\beta\sqrt{2u}$ $(\alpha,\beta\in\mathbb{Z})$, 则 $2\parallel\alpha$, 且 $4|\beta$ (当 $N=1$ 时) 或 $2\parallel\beta$ (当 $N=-1$ 时).

证明

$$E=\frac{1}{2}(T+\sqrt{T^2-4N})=\frac{1}{2}\left(\alpha+\beta\sqrt{2u}+\sqrt{\alpha^2+2\beta^2u+2\alpha\beta\sqrt{2u}-4N}\right),$$

由于 K 是四次循环域, 所以存在 $Y\in\mathbb{Z}$ 使得

$$(\alpha^2+2\beta^2u-4N)^2-4\alpha^2\beta^2\cdot 2u=Y^2\cdot 2u, \tag{5.1}$$

从而可知 $2|\alpha$. 记 $\alpha=2a$, 代入 (8) 式得

$$(4a^2+2\beta^2u-4N)^2-16a^2\beta^2\cdot 2u=2Y^2u, \tag{5.2}$$

所以有 $4|2Y^2u$, $2|Y$, $8|2Y^2u$, 进而有 $8|(4a^2+2\beta^2u-4N)^2$. 故有 $4|2\beta^2u$, $2|\beta$. 记 $\beta=2b$, 代入 (5.2) 式得

$$(4a^2+8b^2u-4N)^2-128a^2b^2u=2Y^2u, \tag{5.3}$$

因而有 $16|2Y^2u,\ 4|Y,\ 32|2Y^2u$, 所以 $32|(4a^2+8b^2u-4N)^2,\ 2|(a^2-N), a$ 为奇数, 即 $2\parallel \alpha$.

$N=1$ 时, $4a^2-4N\equiv 0 \pmod{32}$, (5.3) 式的左端 $\equiv 0 \pmod{64}$, 所以 $8|Y,\ (4a^2+8b^2u-4N)^2\equiv 0 \pmod{128},\ 2|b$.

$N=-1$ 时, $4a^2-4N\equiv 8 \pmod{32}$, 若 $2|b$, 则 (5.3) 式左端 $\equiv 64 \pmod{128}$, $64\parallel 2Y^2u$, 矛盾, 所以 $2\nmid b$.

定理 1.1 的证明 沿用引理中的记号, 记 $T=2a+2b\sqrt{2u}$, 则 $Z=NT^2=4N(a^2+2b^2u+2ab\sqrt{2u})$,

$$\begin{aligned}
R_2^-&\equiv\frac{2}{Q}\cdot\frac{1}{4}\bigg(-8N(a^2+2b^2u+2ab\sqrt{2u})-\frac{1}{6}\cdot4^2(a^2+2b^2u+2ab\sqrt{2u})^2\\
&\qquad+\frac{7}{9}\cdot4^3(a^2+2b^2u+2ab\sqrt{2u})^3+\frac{1}{8}\cdot4^4(a^2+2b^2u+2ab\sqrt{2u})^4\bigg)\ \left(\mathrm{mod}\ \frac{64}{Q}\right)\\
&\equiv\frac{2}{Q}\bigg(-2N(a^2+2b^2u+2ab\sqrt{2u})-\frac{2}{3}(a^2+2b^2u+2ab\sqrt{2u})^2\\
&\qquad+\frac{7}{9}\cdot16(a^2+2b^2u+2ab\sqrt{2u})^3+8(a^2+2b^2u+2ab\sqrt{2u})^4\bigg)\ \left(\mathrm{mod}\ \frac{64}{Q}\right)\\
&\equiv\frac{2}{Q}\bigg(-2N(a^2+2b^2u+2ab\sqrt{2u})-\frac{2}{3}(a^2+2b^2u+2ab\sqrt{2u})^2+\frac{7}{9}\cdot16+8\bigg)\ \left(\mathrm{mod}\ \frac{64}{Q}\right)\\
&\equiv\frac{2}{Q}(-2N(a^2+2b^2u+2ab\sqrt{2u})-22(a^2+2b^2u+2ab\sqrt{2u})^2+16+8)\ \left(\mathrm{mod}\ \frac{64}{Q}\right)\\
&\equiv\frac{2}{Q}(-2N(a^2+2b^2u+2ab\sqrt{2u})+10(a^4+4b^4u^2+12a^2b^2u+4a^3b\sqrt{2u}+8ab^3u\sqrt{2u})+24)\\
&\qquad\left(\mathrm{mod}\ \frac{64}{Q}\right)\\
&\equiv\frac{2}{Q}(-2N(a^2+2b^2u+2ab\sqrt{2u})+10(1+4b^4+12b^2+4ab\sqrt{2u}+8b^3\sqrt{2u})+24)\\
&\qquad\left(\mathrm{mod}\ \frac{64}{Q}\right)\\
&\equiv\frac{2}{Q}(2-2N(a^2+2b^2u+2ab\sqrt{2u})+10(4b^4+12b^2+4ab\sqrt{2u}+8b^3\sqrt{2u}))\ \left(\mathrm{mod}\ \frac{64}{Q}\right).\\
&\equiv\frac{2}{Q}(2-2N(a^2+2b^2u+2ab\sqrt{2u})+8ab\sqrt{2u}+16b^3\sqrt{2u})\ \left(\mathrm{mod}\ \frac{64}{Q}\right),
\end{aligned}$$

$N=1$ 时, $2|b$, 从而有

$$R_2^-\equiv\frac{2}{Q}(2-2(a^2+2b^2)+4ab\sqrt{2u})\ \left(\mathrm{mod}\ \frac{64}{Q}\right).$$

代入类数同余公式 (3.7) 可得,

$$h^-\frac{2}{Q}(2-2a^2-4b^2+4ab\sqrt{2u})\equiv 8F_1\tilde{h}^- \pmod{32}.$$

由于 2 在 $\mathbb{Q}_2(\sqrt{2u})$ 中分歧, $\mathbb{Q}(\sqrt{2u})\cap 2O_{\mathbb{Q}_2(\sqrt{2u})}=2O_{\mathbb{Q}(\sqrt{2u})}$, 所以上面的同余式在 $\mathbb{Q}(\sqrt{2u})$ 中成立, 从而可得

$$\begin{cases} h^-\cdot\dfrac{2}{Q}(2-2a^2-4b^2)\equiv 8F_1\tilde{h}^- \pmod{32},\\[2mm] h^-\cdot\dfrac{2}{Q}\cdot 4ab\equiv 0 \pmod{32}.\end{cases}$$

$Q=1$ 时,

$$\begin{cases} h^-(1-a^2-2b^2)\equiv 2F_1\tilde{h}^- \pmod 8, \\ h^-\cdot ab\equiv 0 \pmod 4, \end{cases}$$

即

$$\begin{cases} \tilde{h}^-\equiv 0 \pmod 4, \\ bh^-\equiv 0 \pmod 4. \end{cases}$$

$Q=2$ 时,

$$\begin{cases} h^-(1-a^2-2b^2)\equiv 4F_1\tilde{h}^- \pmod{16}, \\ h^-\cdot ab\equiv 0 \pmod 8, \end{cases}$$

即

$$\begin{cases} bh^-\equiv 0 \pmod 8, \\ (1-a^2)h^-\equiv 4\tilde{h}^- \pmod{16}. \end{cases}$$

$N=-1$ 时, $2\nmid b$, 从而有

$$\begin{aligned} R_2^- &\equiv \frac{2}{Q}(2+2(a^2+2b^2u+2ab\sqrt{2u})+8ab\sqrt{2u}+16\sqrt{2u}) \left(\mathrm{mod}\frac{64}{Q}\right) \\ &\equiv \frac{2}{Q}(2+2a^2+4u+12ab\sqrt{2u}+16\sqrt{2u}) \left(\mathrm{mod}\frac{64}{Q}\right). \end{aligned}$$

代入类数同余公式 (3.7) 得

$$h^-\cdot\frac{2}{Q}(2+2a^2+4u+12ab\sqrt{2u}+16\sqrt{2u})\equiv 8F_1\tilde{h}^- \pmod{32}.$$

$Q=1$ 时,

$$\begin{cases} h^-(1+a^2+2u)\equiv 2F_1\tilde{h}^- \pmod 8, \\ h^-(6ab+8b)\equiv 0 \pmod 8, \end{cases}$$

即

$$\begin{cases} h^-(1+u)\equiv F_1\tilde{h}^- \pmod 4, \\ h^-\equiv 0 \pmod 4, \end{cases}$$

即

$$h^-\equiv 0 \pmod 4, \qquad \tilde{h}^-\equiv 0 \pmod 4.$$

$Q=2$ 时,

$$\begin{cases} h^-(1+a^2+2u)\equiv 4F_1\tilde{h}^- \pmod{16}, \\ h^-(6ab+8b)\equiv 0 \pmod{16}, \end{cases}$$

由下面的式子得

$$h^-\equiv 0 \pmod 8,$$

代入上面的式子得

$$4F_1\tilde{h}^-\equiv 0 \pmod{16},$$

即

$$\tilde{h}^- \equiv 0 \pmod 4.$$

5.2 $8\|F$ 的情形

先讨论 K/k 的 2-adic 整基. 因为假设 $f \equiv 5 \pmod 8$, 所以 2 在 k 中惯性. 当 $2 \nmid \theta$ 时, $v_2(\mathrm{Disc}(1,\sqrt{\theta})) = v_2(4\theta) = v_2(4)$, 因为 $4|(F/f)$, 所以 $\{1,\sqrt{\theta}\}$ 是 K/k 的 2-adic 整基, 所以对于任意的 $\alpha \in O_K$, 存在 2-adic 整数 x, y 使得 $\alpha = x + y\sqrt{\theta}$. 当 $2|\ \theta$ 时, 由局部域的完全分歧扩张理论可知, $\{1,\sqrt{\theta}\}$ 仍为 K/k 的 2-adic 整基. 设 $E = x + y\sqrt{\theta},\ x, y \in k$ 是 2-adic 整数, 则 $T = 2x,\ v_2(T) \geqslant 1$. 因为 2 在 k 中惯性, 而 k 的一组整基为 $\{1,\ \frac{1+\sqrt{f}}{2}\}$, 所以可设 $T = 2(a + b\frac{1+\sqrt{f}}{2}) = (2a+b) + b\sqrt{f}\ (a, b \in \mathbb{Z})$.

下面计算 R_2^-, 进而证明定理 1.2. 记 $a + b\frac{1+\sqrt{f}}{2} = T_1$, $\frac{1+\sqrt{f}}{2} = v$, 则 $v^2 = v + \frac{f-1}{4}$. 记 $\frac{f-1}{4} = g$. 因为 $f \equiv 5 \pmod 8$, 所以 $g \equiv 1 \pmod 2$.

$$\begin{aligned}
T_1^2 &= a^2 + b^2v^2 + 2abv = (a^2 + b^2g) + b(2a+b)v,\\
T_1^4 &= (a^2 + b^2g)^2 + b^2(2a+b)^2v^2 + 2b(2a+b)(a^2+b^2g)v\\
&= a^4 + 2a^2b^2g + b^4g^2 + b^2(2a+b)^2g + b(2a+b)(2ab + b^2 + 2a^2 + 2b^2g)v\\
&\equiv a^4 + 2a^2b^2g + b^4 + b^2(2a+b)^2g + b(2a+b)(2ab + b^2 + 2a^2 + 2b^2g)v \pmod 8\\
&\equiv a^2 + b^2v \pmod 2,\\
T_1^8 &\equiv a^4 + 2a^2b^2v + b^4v^2 \pmod 4\\
&\equiv a^2 + b^2(g+v) + 2a^2b^2v \pmod 4\\
&\equiv a^2 + b^2(g+v) + 2a^2b^2v \pmod 4\\
&\equiv a^2 + b^2g + (2a^2+1)b^2v \pmod 4.
\end{aligned}$$

代入 R_2^- 的同余表达式得

$$\begin{aligned}
R_2^- &\equiv \frac{2}{Q}\cdot\frac{1}{4}\bigg(-2N\cdot 4NT_1^2 - \frac{1}{6}(4NT_1^2)^2 + \frac{7}{9}(4NT_1^2)^3 + \frac{1}{8}(4NT_1^2)^4\bigg) \pmod{32}\\
&\equiv \frac{2}{Q}(-2T_1^2 - 6T_1^4 + 8T_1^8) \left(\bmod\ \frac{32}{Q}\right)\\
&\equiv \frac{2}{Q}(-2a^2 - 2b^2g - 2b(2a+b)v\\
&\quad - 6(a^4 + 2a^2b^2g + b^4 + b^2(2a+b)^2g + b(2a+b)(2ab + b^2 + 2a^2 + 2b^2g)v)\\
&\quad + 8(a^2 + b^2g + 2a^2b^2v + b^2v)) \left(\bmod\ \frac{32}{Q}\right)\\
&\equiv \frac{2}{Q}(2a^2(1-a^2) + 2b^2(2a^2g-3) + (4ab(1-ab) + 2b^2(2g-1-3b^2))v)\left(\bmod\ \frac{32}{Q}\right),
\end{aligned}$$

代入类数同余公式 (3.8) 得

$$\begin{aligned}
&h^-\frac{2}{Q}(2a^2(1-a^2) + 2b^2(2a^2g-3)\\
&\qquad + (4ab(1-ab) + 2b^2(2g-1-3b^2))v) \equiv 4F_1\tilde{h}^- \pmod{16},\\
&h^-(a^2(1-a^2) + b^2(2a^2g-3)\\
&\qquad + (2ab(1-ab) + b^2(2g-1-3b^2))v) \equiv QF_1\tilde{h}^- \pmod{4Q},
\end{aligned}$$

$$\begin{cases} h^-(a^2(1-a^2)+b^2(2a^2g-3)) \equiv QF_1\tilde{h}^- \pmod{4Q}, \\ h^-(2ab(1-ab)+b^2(2g-1-3b^2)) \equiv 0 \pmod{4Q}, \end{cases}$$

即

$$\begin{cases} h^-\left(a^2(1-a^2)+b^2\left(\dfrac{f-1}{2}a^2-3\right)\right) \equiv QF_1\tilde{h}^- \pmod{4Q}, \\ h^-\left(2ab(1-ab)+b^2\left(\dfrac{f-1}{2}-1-3b^2\right)\right) \equiv 0 \pmod{4Q}. \end{cases}$$

5.3 $4\|F$ 的情形

与 5.2 节类似讨论, 可知,

$$\begin{aligned} T_1^2 &= a^2+b^2v^2+2abv = (a^2+b^2g)+b(2a+b)v, \\ T_1^4 &= (a^2+b^2g)^2+b^2(2a+b)^2v^2+2b(2a+b)(a^2+b^2g)v \\ &\equiv a^2+2a^2b^2+b^2(1+g)+b^2(2a^2+3)v \pmod 4. \end{aligned}$$

代入 R_2^- 的同余表达式得:

$$\begin{aligned} R_2^- &\equiv \frac{2}{Q}(-2T_1^2-6T_1^4) \left(\mathrm{mod}\ \frac{16}{Q}\right) \\ &\equiv \frac{2}{Q}(-2a^2-2b^2g-2b(2a+b)v-6(a^2+2a^2b^2+b^2(1+g)+b^2(2a^2+3)v))\left(\mathrm{mod}\ \frac{16}{Q}\right) \\ &\equiv \frac{2}{Q}(4a^2b^2+2b^2+4b^2v)\left(\mathrm{mod}\ \frac{16}{Q}\right). \end{aligned}$$

代入类数同余公式 (3.9) 得:

$$h^-\frac{2}{Q}(4a^2b^2+2b^2+4b^2v) \equiv 4\tilde{h}^- \pmod 8,$$

$$\begin{cases} h^-(2a^2b^2+b^2) \equiv QF_1\tilde{h}^- \pmod{2Q}, \\ b^2h^- \equiv 0 \pmod{Q}. \end{cases}$$

即

$$b^2h^- \equiv 0 \pmod{Q}, \quad b^2h^- \equiv Q\tilde{h}^- \pmod{2Q}.$$

5.4 $2\nmid F$ 的情形

此时, 假设 $v_2(T) \geqslant 1$. 因为 $f \equiv 5 \pmod 8$, 2 在 k 中惯性, 所以 $T = 2(a+b\frac{1+\sqrt{f}}{2}) = (2a+b)+b\sqrt{f}$ $(a,b \in \mathbb{Z})$. 与 5.3 节类似讨论可知,

$$\begin{aligned} T_1^2 &= a^2+b^2v^2+2abv = (a^2+b^2g)+b(2a+b)v. \\ T_1^4 &= (a^2+b^2g)^2+b^2(2a+b)^2v^2+2b(2a+b)(a^2+b^2g)v \\ &\equiv a^2+2a^2b^2+b^2(1+g)+b^2(2a^2+3)v \pmod 4. \end{aligned}$$

代入 R_2^- 的同余表达式得:

$$\begin{aligned} R_2^- &\equiv \frac{2}{Q}(-2T_1^2-6T_1^4) \left(\mathrm{mod}\ \frac{16}{Q}\right) \\ &\equiv \frac{2}{Q}(-2a^2-2b^2g-2b(2a+b)v-6(a^2+2a^2b^2+b^2(1+g)+b^2(2a^2+3)v)) \left(\mathrm{mod}\ \frac{16}{Q}\right) \end{aligned}$$

$$\equiv \frac{2}{Q}(4a^2b^2 + 2b^2 + 4b^2v) \left(\bmod \frac{16}{Q}\right).$$

代入类数同余公式 (3.10) 得

$$h^- \frac{2}{Q}(4a^2b^2 + 2b^2 + 4b^2v) \equiv 2\tilde{h}^- \pmod 8,$$

$$\begin{cases} h^-(4a^2b^2 + 2b^2) \equiv QF_1\tilde{h}^- \pmod{4Q}, \\ b^2h^- \equiv 0 \pmod Q, \end{cases}$$

即

$$b^2h^- \equiv 0 \pmod Q, \quad 2b^2h^- \equiv QF_1\tilde{h}^- \pmod{4Q}.$$

参考文献

1 Ankeny N, Artin E, Chowla S. The class number of quadratic number fields. *Ann of Math*, **52**(2): 479–493 (1952)

2 Lu H W. Congruences for the class number of quadratic fields. *Abh Math Sen Univ Hamberg*, **47**: 254–258 (1983)

3 Feng K. Ankeny-Artin-Chowla formula on cubic cyclic number fields. *J Univ Sci Tech China*, **12**: 20–27 (1982)

4 Zhang X. Congruences of class numbers of general cubic cyclic number fields. *J Univ Sci Tech China*, **17**(2): 141–145 (1987)

5 Zhang X. Ten formulae of type Ankeny-Artin-Chowla for class numbers of general cyclic quartic fields. *Sci China Ser A-Math*, **32**(4): 417–428 (1989)

6 Liu T. Congruence for the class numbers of real cyclic sextic number fields. *Sci China Ser A-Math*, **42**(10): 1009–1018 (1999)

7 Zhang X. Congruence modulo 8 for the class numbers of general quadratic fields $\mathbb{Q}(\sqrt{m})$ and $\mathbb{Q}(\sqrt{-m})$. *J Number Theory*, **32**(3): 332–338 (1989)

8 Hasse H. Arithmetische Bestimmung von Grundeinheit und Klassenzahl in zyklischen kubischen und biquadratischen Zahlkörpern. *Abh Deutsch Akad Wiss Berlin Math*, **2**: 1–95 (1948)

9 Lazarus A J. On the class number and unit index of simplex quartic fields. *Nagoya Math J*, **121**: 1–13 (1991) (1989)

10 Feng K. Explicit description of quartic cyclic numberfields. *Acta Math Sinica*, **27**(3): 410–424 (1984)

11 张贤科. 代数数论导引. 长沙: 湖南教育出版社, 1999

12 Washington L C. Introduction to Cyclotomic Fields. Berlin: Spring-Verlag, 1982

13 Kudo A. On a class number relation of imaginary abelian fields. *J Math Soc Japan*, **27**(1): 150–159 (1975)

14 Shiratani K. Kummer's congruence for generalized Bernoulli numbers and its application. *Mem Fac Sci Kyushu Univ*, **26**: 119–138 (1972)