关于四次剩余符号与互反律的注记*

孙智宏
(淮阴师专)

NOTES ON QUARTIC RESIDUE SYMBOL AND RATIONAL RECIPROCITY LAWS

Sun Zhihong
(Huaiyin Normal College)

Abstract

In section 2 of this paper, we solve completely the rational quartic residue problem. Section 3 is devoted to giving elementary proofs of Burde's reciprocity law and Schdz's reciprocity law.

§1 引 言

设 p,q 是不同的奇素数，著名的二次互反律指出

$$\left(\frac{2}{p}\right)=\left(-1\right)^{\frac{p^2-1}{8}},\qquad \left(\frac{-1}{p}\right)=(-1)^{\frac{p-1}{2}},$$
$$\left(\frac{p}{q}\right)=(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}\left(\frac{q}{p}\right)$$

这里 $(\cdot)$ 为 Legendre 符号．

在 Gauss 整数环 $\mathbb{Z}[i]$ 中考虑四次剩余问题．对 Gauss 整数 $a+bi(a,b\in\mathbb{Z})$，它的范为 $N(a+bi)=a^2+b^2$．若 $a\equiv1(\bmod 4),b\equiv0(\bmod 4)$ 或 $a\equiv3(\bmod 4),b\equiv2(\bmod 4)$，则称 $a+bi$ 是本原数，若 $\pi\in\mathbb{Z}[i]$ 除去单位因子外仅有与它相伴的因子，则称 π 为不可分数 (Gauss 素数)．

对 $\pi,\lambda\in\mathbb{Z}[i],(1+i)\nmid\pi$，四次剩余符号 $\chi_\pi(\lambda)=(\frac{\lambda}{\pi})_4$ 如 [1] 所定义，当 $\pi=a+bi,\lambda=c+di$ 是互素的本原数时，我们有如下的 Eisenstein 四次互反律：

$$\left(\frac{\lambda}{\pi}\right)_4=(-1)^{\frac{N(\pi)-1}{4}\cdot\frac{N(\lambda)-1}{4}}\left(\frac{\pi}{\lambda}\right)_4=(-1)^{\frac{a-1}{2}\cdot\frac{c-1}{2}}\left(\frac{\pi}{\lambda}\right)_4$$

设 $p=\pi\bar{\pi}$ 是 $4k+1$ 形素数，$a\in\mathbb{Z}$，$(\frac{a}{p})=1$，易见同余式 $x^4\equiv a(\bmod p)$ 有有理整数解

* 1990年6月29日收到．

的充分必要条件是 $\left(\frac{a}{\pi}\right)_4=1$. 1969 年 K.Burde[2] 发现下面的互反律:若 $p=\pi\bar{\pi},q=\lambda\bar{\lambda}$ 是不同的 $4k+1$ 形素数,$\left(\frac{p}{q}\right)=1$,则

$$\left(\frac{q}{\pi}\right)_4\left(\frac{p}{\lambda}\right)_4=(-1)^{\frac{q-1}{4}}\left(\frac{ad-bc}{q}\right)$$

其中 a,b,c,d 由 $p=a^2+b^2$, $q=c^2+d^2$, $a\equiv c\equiv 1(\mathrm{mod}2)$ 确定.

Burde 互反律又称为有理的四次互反律.被认为是独立于 Eisenstein 四次互反律的重要结果.

设 p,q 是不同的 $4k+1$ 形素数,$\varepsilon_p,\varepsilon_q$ 分别是二次域 $Q(\sqrt{p})$、$Q(\sqrt{q})$ 的基本单位,A.Scholz[3] 在 1934 年用类域论的方法证明

$$\left(\frac{\varepsilon_p}{q}\right)=\left(\frac{\varepsilon_q}{p}\right)$$

这个互反律被 E Lehmer[4] 重新发现.

本文将利用高次剩余符号化为低次剩余符号计算的技巧给出 $x^4\equiv p(\mathrm{mod}\ q)$ 有解的条件,这里 p 是 $4k+3$ 形素数,q 是 $4k+1$ 形素数,$(\frac{p}{q})=1$. 同时说明 Burde 互反律.Scholz 互反律分别是四次互反律和二次互反律的推论.

§2 剩余符号的转换及其应用

设 m 为正奇数,$(\frac{n}{m})$ 表示 n 对 m 的 Jacobi 符号.

命题1 设 m 为正奇数,$a,b\in\mathbb{Z}$,$(a^2+b^2,m)=1$,则

$$\left(\frac{a+bi}{m}\right)_4^2=\left(\frac{a^2+b^2}{m}\right)$$

证明 由于 $(\frac{\cdot}{m})_4$ 与 $(\frac{\cdot}{m})$ 是完全积性函数,而

$$(a+bi)(c+di)=(ac-bd)+(bc+ad)i,$$
$$(a^2+b^2)(c^2+d^2)=(ac-bd)^2+(bc+ad)^2$$

故仅需对 $(\frac{1+i}{q})_4^2$、$(\frac{a+bi}{q})_4^2$ 证明命题.这里 $a^2+b^2=p$ 与 q 是不同的奇素数.

设与 $a+bi$ 相伴的本原数是 a_1+b_1i,与 q 相伴的本原数是 q_1,则

$$\left(\frac{1+i}{q}\right)_4^2=\left(\frac{1+i}{q_1}\right)_4^2=\left(i^{\frac{q_1-1}{4}}\right)^2=(-1)^{\frac{q_1-1}{4}}=\left(\frac{2}{|q_1|}\right)=\left(\frac{2}{q}\right),$$

$$\left(\frac{a+bi}{q}\right)_4^2=\left(\frac{a_1+b_1i}{q_1}\right)_4^2=\left(\frac{q_1}{a_1+b_1i}\right)_4^2\equiv q_1^{2\cdot\frac{p-1}{4}}\equiv\left(\frac{q_1}{p}\right)=\left(\frac{q}{p}\right)=\left(\frac{p}{q}\right)$$

故命题得证.

令 $u_n(a,b)$ 表示如下定义的 Lucas 序列．

$$u_0(a,b)=0,\qquad u_1(a,b)=1,\cdots,u_{k+1}(a,b)=bu_k(a,b)-au_{k-1}(a,b).$$

则熟知

$$u_n(a,b)=\frac{1}{\sqrt{b^2-4a}}\left\{\left(\frac{b+\sqrt{b^2-4a}}{2}\right)^n-\left(\frac{b-\sqrt{b^2-4a}}{2}\right)^n\right\}$$

现在我们可以给出四次剩余符号与二次剩余符号的一些转换关系．

定理 1 设 $b,c\in\mathbb{Z}$，p 为奇素数，则

(1) 当 $\left(\frac{b^2-c^2}{p}\right)=1$ 且 $p\nmid c(b+c)$ 时，$\left(\frac{b+c}{p}\right)=\left(\frac{2}{p}\right)\left(\frac{b+\sqrt{b^2-c^2}}{p}\right)$

(2) 当 $p\equiv 3(\bmod 4)$，$p\nmid c$ 且 $\left(\frac{b^2+c^2}{p}\right)=1$ 时，

$$\left(\frac{b+ci}{p}\right)_4=\left(\frac{2\sqrt{b^2+c^2}}{p}\right)\left(\frac{b+\sqrt{b^2+c^2}}{p}\right)$$

(3) 当 $p\equiv 3(\bmod 4)$ 且 $\left(\frac{b^2+c^2}{p}\right)=-1$ 时，

$$\left(\frac{b+ci}{p}\right)_4=-\left(\frac{2c\sqrt{-b^2-c^2}}{p}\right)\left(\frac{b+\sqrt{-b^2-c^2}\,i}{p}\right)_4=i\left(\frac{2c}{p}\right)\left(\frac{u_{\frac{p+1}{2}}\left(-\frac{c^2}{4},b\right)}{p}\right)$$

其中 $\sqrt{t}$ 理解为取定的 $x^2\equiv t(\bmod p)$ 的一个解．

证明 (1) 由于 $(b+c)\left(\frac{b+\sqrt{b^2-c^2}}{2}\right)=\left(\frac{b+c+\sqrt{b^2-c^2}}{2}\right)^2$，故当 $p\nmid(b+c+\sqrt{b^2-c^2})$ 即 $p\nmid c(b+c)$ 时 $\left(\frac{b+c}{p}\right)=\left(\frac{2}{p}\right)\left(\frac{b+\sqrt{b^2-c^2}}{p}\right)$.

(2) 因 $(b+ci)\cdot\frac{b+\sqrt{b^2+c^2}}{2}=\left(\frac{b+ci+\sqrt{b^2+c^2}}{2}\right)^2$，故

$$(b+ci)^{\frac{p^2-1}{4}}\cdot\left(\frac{b+\sqrt{b^2+c^2}}{2}\right)^{\frac{p+1}{4}\cdot p-1}=\left(\frac{b+\sqrt{b^2+c^2}+ci}{2}\right)^{\frac{p^2-1}{2}}.$$

由四次剩余符号定义和命题 1 及 $p\nmid c$ 得

$$\left(\frac{b+ci}{p}\right)_4=\left(\frac{(b+\sqrt{b^2+c^2}+ci)/2}{p}\right)_4^2=\left(\frac{(b+\sqrt{b^2+c^2})^2+c^2}{p}\right)$$

$$=\left(\frac{2(b^2+c^2)+2b\sqrt{b^2+c^2}}{p}\right)=\left(\frac{2\sqrt{b^2+c^2}}{p}\right)\left(\frac{b+\sqrt{b^2+c^2}}{p}\right).$$

(3) 由 $(b+ci)\cdot\frac{b+\sqrt{-b^2-c^2}\,i}{2}=\left(\frac{b+ci+\sqrt{-b^2-c^2}\,i}{2}\right)^2$ 知

$$\left(\frac{b+ci}{p}\right)_4\left(\frac{(b+\sqrt{-b^2-c^2}i)/2}{p}\right)_4\equiv(b+ci)^{\frac{p^2-1}{4}}\cdot\left(\frac{b+\sqrt{-b^2-c^2}i}{2}\right)^{\frac{p^2-1}{4}}$$

$$=\left(\frac{b+ci+\sqrt{-b^2-c^2}i}{2}\right)^{\frac{p^2-1}{2}}$$

$$\equiv\left(\frac{(b+ci+\sqrt{-b^2-c^2}i)/2}{p}\right)_4^2=\left(\frac{b^2+(c+\sqrt{-b^2-c^2})^2}{p}\right)$$

$$=\left(\frac{2c\sqrt{-b^2-c^2}}{p}\right)$$

而 $p\nmid c$, $\left(\frac{(b+\sqrt{-b^2-c^2}i)/2}{p}\right)_4^2=\left(\frac{b^2+(-b^2-c^2)}{p}\right)=-1$, 故

$$\left(\frac{b+ci}{p}\right)_4=-\left(\frac{2c\sqrt{-b^2-c^2}}{p}\right)\left(\frac{(b+\sqrt{-b^2-c^2}i)/2}{p}\right)_4$$

$$=\left(\frac{-2c\sqrt{-b^2-c^2}}{p}\right)\left(\frac{b+\sqrt{-b^2-c^2}i}{p}\right)_4$$

因 $\left(\frac{b^2+c^2}{p}\right)=-1$; $\left(\frac{-c^{2/4}}{p}\right)=-1$, $(m+ni)^p\equiv m-ni(\bmod p)$, 故

$$u_{\frac{p+1}{2}}\left(\frac{-c^2}{4},b\right)=\frac{1}{\sqrt{b^2+c^2}}\left\{\left(\frac{b+\sqrt{b^2+c^2}}{2}\right)^{\frac{p+1}{2}}-\left(\frac{b-\sqrt{b^2+c^2}}{2}\right)^{\frac{p+1}{2}}\right\}$$

$$=\frac{1}{\sqrt{b^2+c^2}}\left(\frac{b-\sqrt{b^2+c^2}}{2}\right)^{\frac{p+1}{2}}\left\{\left(\frac{b+\sqrt{b^2+c^2}}{b-\sqrt{b^2+c^2}}\right)^{\frac{p+1}{2}}-1\right\}$$

$$=\frac{1}{\sqrt{b^2+c^2}}\left(\frac{b-\sqrt{b^2+c^2}}{2}\right)^{\frac{p+1}{2}}\left\{\frac{b+\sqrt{b^2+c^2}}{c}\cdot\frac{(b+\sqrt{b^2+c^2})^p}{c^p}-1\right\}$$

$$\equiv\frac{1}{\sqrt{-b^2-c^2}i}\left(\frac{b-\sqrt{-b^2-c^2}i}{2}\right)^{\frac{p+1}{2}}\left(\frac{b+\sqrt{-b^2-c^2}i}{c}\cdot\frac{b-\sqrt{-b^2-c^2}i}{c}\right.$$
$$\left.-1\right)$$

$$=\frac{1}{\sqrt{-b^2-c^2}i}\left(\frac{b-\sqrt{-b^2-c^2}i}{2}\right)^{\frac{p+1}{2}}\cdot(-2)\equiv\frac{i}{\sqrt{-b^2-c^2}}\left(\frac{2}{p}\right)(b$$
$$-\sqrt{-b^2-c^2}i)^{\frac{p+1}{2}}(\bmod p)$$

由此

$$\left(\frac{u_{\frac{p+1}{2}}(-\frac{c^2}{4},b)}{p}\right)\equiv\left[u_{\frac{p+1}{2}}(-\frac{c^2}{4},b)\right]^{\frac{p-1}{2}}\equiv\frac{i^{\frac{p-1}{2}}(\frac{2}{p})^{\frac{p-1}{2}}}{(\sqrt{-b^2-c^2})^{\frac{p-1}{2}}}(b-\sqrt{b^2-c^2}i)^{\frac{p^2-1}{4}}$$

$$\equiv -i\left(\frac{\sqrt{-b^2-c^2}}{p}\right)\cdot\left(\frac{b-\sqrt{-b^2-c^2}\,i}{p}\right)_4 (\mathrm{mod} p).$$

从而

$$\left(\frac{b+ci}{p}\right)_4=\left(\frac{2c\sqrt{-b^2-c^2}}{p}\right)\left(\frac{b-\sqrt{-b^2-c^2}\,i}{p}\right)_4=i\left(\frac{2c}{p}\right)\left(\frac{u_{\frac{p+1}{2}}(-\frac{c^2}{4},b)}{p}\right).$$

综上定理得证.

根据定理 1, 我们可彻底解决有理四次剩余问题.

显然有理四次剩余问题可简化为同余方程

$$x^4\equiv p \qquad (\mathrm{mod} q)$$

的可解性研究, 这里 p,q 是不同素数, $q\equiv 1(\mathrm{mod}4)$, $\left(\frac{p}{q}\right)=1$.

当 $p=2$ 时, 已知 $x^4\equiv 2(\mathrm{mod} q)$ 可解当且仅当 q 可表成 A^2+64B^2([1]P.64). 当 p 是 $4k+1$ 形素数时, 由 Burde 互反律不难确定 $x^4\equiv p(\mathrm{mod} q)$ 的可解性. 当 p 是 $4k+3$ 形素数时, 我们有

定理 2 设 p 是 $4k+3$ 形素数, q 是 $4k+1$ 形素数, $\left(\frac{p}{q}\right)=1, q=b^2+c^2, 2|c$, 则

(i) 当 $p|c$ 时, $x^4\equiv p(\mathrm{mod} q)$ 可解 $\Leftrightarrow q\equiv 1(\mathrm{mod}8)$

(ii) 当 $p|b$ 时, $x^4\equiv p(\mathrm{mod} q)$ 可解 $\Leftrightarrow q\equiv p+2(\mathrm{mod}8)$

(iii) 当 $p\nmid bc$ 时, $x^4\equiv p(\mathrm{mod} q)$ 可解 $\Leftrightarrow\left(\frac{b+\sqrt{q}}{p}\right)=(-1)^{\frac{q-1}{4}}$, 其中 $\sqrt{q}$ 满足 $\left(\frac{\sqrt{q}}{p}\right)=(-1)^{\frac{p+1}{4}}$.

证明 我们先证明 $x^4\equiv p(\mathrm{mod} q)$ 可解 $\Leftrightarrow\left(\frac{b+ci}{p}\right)_4=(-1)^{\frac{q-1}{4}}$.

若 $x^4\equiv p(\mathrm{mod} q)$, 则 $x^4\equiv p(\mathrm{mod} b+ci)$, 从而 $\left(\frac{p}{b+ci}\right)_4=1$.

若 $\left(\frac{p}{b+ci}\right)_4=1$, 则存在 $m,n\in\mathbb{Z}$ 使 $(m+ni)^4\equiv p(\mathrm{mod} b+ci)$. 于是

$$\left(\frac{mc-nb}{c}\right)^4\equiv\left(\frac{mc+nci}{c}\right)^4=(m+ni)^4\equiv p(\mathrm{mod}\ b+ci).$$

令 $t\equiv\frac{mc-nb}{c}(\mathrm{mod} q)$, 则 $t^4\equiv p(\mathrm{mod} b+ci)$, 因而

$$q=N(b+ci)|(t^4-p)^2, \qquad t^4\equiv p(\mathrm{mod} q).$$

故 $x^4\equiv p(\mathrm{mod} q)$ 可解当且仅当 $\left(\frac{p}{b+ci}\right)_4=1$, 但

$$\left(\frac{p}{b+ci}\right)_4=1\Leftrightarrow(-1)^{\frac{q-1}{4}}\left(\frac{-p}{b+ci}\right)_4=1\Leftrightarrow(-1)^{\frac{q-1}{4}}\left(\frac{b+ci}{-p}\right)_4=1$$

$$\Leftrightarrow\left(\frac{b+ci}{4}\right)_4=(-1)^{\frac{q-1}{4}}$$

故必 $x^4\equiv p(\bmod q)$ 可解 $\Leftrightarrow\left(\frac{b+ci}{p}\right)_4=(-1)^{\frac{q-1}{4}}$.

(i) 当 $p|c$ 时, $\left(\frac{b+ci}{p}\right)_4=\left(\frac{b}{p}\right)_4\equiv b^{\frac{p+1}{4}\cdot(p-1)}\equiv 1(\bmod p)$, 故此时 $x^4\equiv p(\bmod q)$ 可解当且仅当 $q\equiv 1(\bmod 8)$.

(ii) 当 $p|b$ 时, $\left(\frac{b+ci}{p}\right)_4=\left(\frac{ci}{p}\right)_4=i^{\frac{p^2-1}{4}}\left(\frac{c}{p}\right)_4=(-1)^{\frac{p^2-1}{8}}=(-1)^{\frac{p+1}{4}}$, 故

$$x^4\equiv p(\bmod q)\text{可解}\Leftrightarrow(-1)^{\frac{p+1}{4}}=(-1)^{\frac{q-1}{4}}\Leftrightarrow q\equiv p+2(\bmod 8).$$

(iii) 当 $p\nmid bc$ 时, 由定理 1(2) 知 $\left(\frac{\sqrt{q}}{p}\right)=(-1)^{\frac{p+1}{4}}$ 时

$$\left(\frac{b+ci}{p}\right)_4=\left(\frac{2\sqrt{q}}{p}\right)\left(\frac{b+\sqrt{q}}{p}\right)=\left(\frac{b+\sqrt{q}}{p}\right).$$

故 $x^4\equiv p(\bmod q)$ 可解当且仅当 $\left(\frac{b+\sqrt{q}}{p}\right)=(-1)^{\frac{q-1}{4}}$.

于是定理得证.

设 p 是 $4k+3$ 形素数, $a,b\in\mathbb{Z}$, $\left(\frac{a^2+b^2}{p}\right)=1$, 则

$$[(a+bi)^{\frac{p^2-1}{8}}]^4=(a+bi)^{\frac{p^2-1}{2}}\equiv\left(\frac{a+bi}{p}\right)_4^2=\left(\frac{a^2+b^2}{p}\right)=1(\bmod p)$$

故存在 $r\in\{0,1,2,3\}$, 使 $(a+bi)^{\frac{p^2-1}{8}}\equiv i^r(\bmod p)$. 我们定义 $a+bi$ 对 p 的 8 次剩余符号为 $\left(\frac{a+bi}{p}\right)_8=i^r$.

定理 1 的第二个应用就是当 $\left(\frac{a+bi}{p}\right)_4=1$ 时确定 $\left(\frac{a+bi}{p}\right)_8$. 为此先有

引理 1 设 p 为 $4k+3$ 形素数, $2\nmid a,2|b$, $\left(\frac{a^2+b^2}{p}\right)=1$, $\left(\frac{\sqrt{a^2+b^2}}{p}\right)=\left(\frac{a+bi}{p}\right)_4$, 则

$$\left(\frac{a+bi}{p}\right)_8=\left(\frac{\sqrt{\frac{x+a}{2}}+\sqrt{\frac{x-a}{2}}\,i}{p}\right)_4$$

其中 $x=\sqrt{a^2+b^2}$, $\left(\sqrt{\frac{x+a}{2}}\Big/p\right)=1$, $\left(\frac{\sqrt{\frac{x-a}{2}}}{p}\right)=\left(\frac{2b}{p}\right)$.

证明 由于 $x=\sqrt{a^2+b^2}$, $\left(\frac{x}{p}\right)=\left(\frac{a+bi}{p}\right)_4$, 故由定理 1 得

$$\left(\frac{a+bi}{p}\right)_4=\left(\frac{2\sqrt{a^2+b^2}}{p}\right)\left(\frac{a+\sqrt{a^2+b^2}}{p}\right)$$

$$=\left(\frac{2x}{p}\right)\left(\frac{a+x}{p}\right)=\left(\frac{a+bi}{p}\right)_4\left(\frac{(a+x)/2}{p}\right)$$

即 $\left(\frac{(a+x)/2}{p}\right)=1.$

因 $\left(\frac{(a+x)/2}{p}\right)\left(\frac{(x-a)/2}{p}\right)=\left(\frac{b^2/4}{p}\right)=1$, 故 $\left(\frac{(x-a)/2}{p}\right)=1$. 令

$$c^2\equiv\frac{a+x}{2}\bmod p),\left(\frac{c}{p}\right)=1;\quad d^2\equiv\frac{x-a}{2}\pmod p,\left(\frac{d}{p}\right)=\left(\frac{2b}{p}\right).$$

则

$$(c+di)^2=c^2-d^2+2cdi\equiv\left(\frac{x+a}{2}-\frac{x-a}{2}\right)+2\cdot\frac{b}{2}i=a+bi\pmod p$$

从而

$$\left(\frac{a+bi}{p}\right)_8\equiv(c+di)^{\frac{p^2-1}{4}}\equiv\left(\frac{c+di}{p}\right)_4\quad\pmod p$$

引理得证.

定理 3 设 p 为 $4k+3$ 形素数, $a,b\in\mathbb{Z}$, $p\nmid ab$, $\left(\frac{a^2+b^2}{p}\right)=1$, $\left(\frac{a+bi}{p}\right)_4=1$, 则

$$\left(\frac{a+bi}{p}\right)_8=\left(\frac{2b}{p}\right)\left(\frac{b+\sqrt{(a-\sqrt{a^2+b^2})^2+b^2}}{p}\right)$$

其中 $\left(\frac{\sqrt{a^2+b^2}}{p}\right)=1$, $\left(\frac{\sqrt{(a-\sqrt{a^2+b^2})^2+b^2}}{p}\right)=\left(\frac{b}{p}\right)$.

证明 令 $x^2\equiv a^2+b^2\pmod p$, $\left(\frac{x}{p}\right)=1$, 由引理 1, 定理 1 得

$$\left(\frac{a+bi}{p}\right)_8=\left(\frac{\sqrt{\frac{x+a}{2}}+\sqrt{\frac{x-a}{2}}\,i}{p}\right)_4=\left(\frac{2\sqrt{x}}{p}\right)\left(\frac{\sqrt{\frac{x+a}{2}}+\sqrt{x}}{p}\right)$$

$$=\left(\frac{2}{p}\right)\left(\frac{1+\sqrt{\frac{2x}{x+a}}}{p}\right)=\left(\frac{2}{p}\right)\left(\frac{1+\frac{1}{b}\sqrt{2x^2-2xa}}{p}\right)=\left(\frac{2b}{p}\right)\left(\frac{b+\sqrt{(x-a)^2+b^2}}{p}\right)$$

其中 $\left(\frac{\sqrt{\frac{x+a}{2}}}{p}\right)=\left(\frac{\sqrt{x}}{p}\right)=\left(\frac{\sqrt{\frac{2x}{x+a}}}{p}\right)=\left(\frac{b}{p}\right)\left(\frac{\sqrt{2x^2-2xa}}{p}\right)=1.$

定理得证.

§3. Burde 互反律与 Scholz 互反律的简单证明

我们先讨论 Scholz 互反律，说明它可只由二次互反律推出.

设 p,q 是不同的 $4k+1$ 形素数，$x^2-py^2=-4$ 与 $x^2-qy^2=-4$ 的最小解为 (t_p,u_p)、(t_q,u_q)，则二次域 $Q(\sqrt{p})$、$Q(\sqrt{q})$ 的基本单位是 $\varepsilon_p=\frac{t_p+u_p\sqrt{p}}{2}$、$\varepsilon_q=\frac{t_q+u_q\sqrt{q}}{2}$.Scholz 互反律断言

$$\left(\frac{\varepsilon_p}{q}\right)=\left(\frac{\varepsilon_q}{p}\right)$$

只要 $\left(\frac{p}{q}\right)=\left(\frac{q}{p}\right)=1$.

若 $t^2-du^2=-4,d\equiv1(\mathrm{mod}4)$，则易知

当 $d\equiv1(\mathrm{mod}8)$ 时，$8|t$； 当 $d\equiv5(\mathrm{mod}8)$ 时，$2\nmid t$ 或 $4|t,8\nmid t$. 令 $t_p+t_q=2^\alpha(t_1+t_2)$，$2\nmid(t_1+t_2)$，则

$$\left(\frac{t_1+t_2}{q}\right)=\left(\frac{q}{|t_1+t_2|}\right)=\left(qu_q^2/|t_1+t_2|\right)=\left(\frac{pu_p^2+t_q^2-t_p^2}{|t_1+t_2|}\right)$$
$$=\left(\frac{pu_p^2}{|t_1+t_2|}\right)=\left(\frac{p}{|t_1+t_2|}\right)=\left(\frac{t_1+t_2}{p}\right).$$

由此当 $\left(\frac{2}{p}\right)=\left(\frac{2}{q}\right)$ 时，

$$\left(\frac{t_p+t_q}{p}\right)=\left(\frac{2^\alpha}{p}\right)\left(\frac{t_1+t_2}{p}\right)=\left(\frac{2^\alpha}{q}\right)\left(\frac{t_1+t_2}{q}\right)=\left(\frac{t_p+t_q}{q}\right).$$

当 $p\equiv1(\mathrm{mod}8),q\equiv5(\mathrm{mod}8)$ 时，$\left(\frac{2}{p}\right)=1$，$\left(\frac{2}{q}\right)=-1$，$8|t_p$，$\alpha=0$ 或 2，故

$$\left(\frac{t_p+t_q}{p}\right)=\left(\frac{t_1+t_2}{p}\right)=\left(\frac{t_1+t_2}{q}\right)=\left(\frac{2^\alpha}{q}\right)\left(\frac{t_1+t_2}{q}\right)=\left(\frac{t_p+t_q}{q}\right).$$

同理当 $p\equiv5(\mathrm{mod}8)$ 且 $q\equiv1(\mathrm{mod}8)$ 时 $\left(\frac{t_p+t_q}{p}\right)=\left(\frac{t_q+t_p}{q}\right)$.

可见我们总有 $\left(\frac{t_p+t_q}{p}\right)=\left(\frac{t_p+t_q}{q}\right)$.

由定理 1(1) 可得

$$\left(\frac{\varepsilon_p}{q}\right)=\left(\frac{(t_p+u_p\sqrt{p})/2}{q}\right)=\left(\frac{2}{q}\right)\left(\frac{t_p+\sqrt{pu_p^2}}{q}\right)=\left(\frac{2}{q}\right)\left(\frac{t_p+\sqrt{t_p^2+4}}{q}\right)$$
$$=\left(\frac{t_p+\sqrt{-4}}{q}\right)=\left(\frac{t_p+t_q}{q}\right)$$

对称地

$$\left(\frac{\varepsilon_q}{p}\right)=\left(\frac{t_p+t_q}{p}\right)$$

故 $\left(\frac{\varepsilon_p}{q}\right)=\left(\frac{\varepsilon_q}{p}\right)$. 这就证明了 Scholz 互反律 .

下面我们着手从四次互反律推导 Burde 互反律，为此先有

命题 2　设 $a,b,c,d\in\mathbb{Z}$,$2\nmid c,2|d,(c,d)=1,(a^2+b^2,c^2+d^2)=1$, 则

$$\left(\frac{a+bi}{c+di}\right)_4^2=(-1)^{\frac{c^2+d^2-1}{4}}\left(\frac{ad-bc}{c^2+d^2}\right).$$

证明　显然

$$\left(\frac{ad-bc}{c+di}\right)_4^2=\left(\frac{ad+bdi}{c+di}\right)_4^2=\left(\frac{d}{c+di}\right)_4^2\left(\frac{a+bi}{c+di}\right)_4^2$$

而

$$\left(\frac{d}{c+di}\right)_4^2=\left(\frac{i^3}{c+di}\right)_4^2\left(\frac{di}{c+di}\right)_4^2=i^{3\cdot\frac{c^2+d^2-1}{2}}\left(\frac{-c}{c+di}\right)_4^2$$

$$=(-1)^{\frac{c^2+d^2-1}{4}}\left(\frac{c+di}{|c|}\right)_4^2=(-1)^{\frac{c^2+d^2-1}{4}}\left(\frac{c^2+d^2}{|c|}\right)=(-1)^{\frac{c^2+d^2-1}{4}}$$

故

$$\left(\frac{a+bi}{c+di}\right)_4^2=(-1)^{\frac{c^2+d^2-1}{4}}\left(\frac{ad-bc}{c+di}\right)_4^2$$

令 a' 为 $a,a+c^2+d^2$ 中偶数 ,b' 为 $b,b+c^2+d^2$ 中奇数，则由命题 1 与广义的二次互反律得

$$\left(\frac{ad-bc}{c+di}\right)_4^2=\left(\frac{a'd-b'c}{c+di}\right)_4^2=\left(\frac{c+di}{|a'd-b'c|}\right)_4^2=\left(\frac{c^2+d^2}{|a'd-b'c|}\right)=\left(\frac{a'd-b'c}{c^2+d^2}\right)$$

$$=\left(\frac{ad-bc}{c^2+d^2}\right)$$

故

$$\left(\frac{a+bi}{c+di}\right)_4^2=(-1)^{\frac{c^2+d^2-1}{4}}\left(\frac{ad-bc}{c+di}\right)_4^2=(-1)^{\frac{c^2+d^2-1}{4}}\left(\frac{ad-bc}{c^2+d^2}\right)$$

命题得证 .

设 p,q 是不同的 $4k+1$ 形素数 ,$\left(\frac{p}{q}\right)=\left(\frac{q}{p}\right)=1,p=a^2+b^2,q=c^2+d^2,\pi=a+bi,\lambda=c+di$ 为本原不可分数，则由命题 1、命题 2 及四次互反律得

$$\left(\frac{\lambda}{\pi}\right)_4^2\left(\frac{\lambda}{\bar{\pi}}\right)_4^2=\left(\frac{\lambda}{p}\right)_4^2=\left(\frac{q}{p}\right)=1$$

$$\left(\frac{\bar{\lambda}}{\pi}\right)_4\left(\frac{\bar{\pi}}{\lambda}\right)_4=\overline{\left(\frac{\lambda}{\bar{\pi}}\right)}\left(\frac{\bar{\pi}}{\lambda}\right)_4=\left[\overline{\left(\frac{\lambda}{\bar{\pi}}\right)_4}\left(\frac{\lambda}{\bar{\pi}}\right)_4\cdot\left(\frac{\lambda}{\bar{\pi}}\right)_4\left(\frac{\bar{\pi}}{\lambda}\right)_4\right]\Big/\left(\frac{\lambda}{\bar{\pi}}\right)_4^2$$

$$=\left(\frac{\lambda}{\bar{\pi}}\right)_4\left(\frac{\bar{\pi}}{\lambda}\right)_4\cdot\left(\frac{\lambda}{\pi}\right)_4^2=(-1)^{\frac{p-1}{4}\cdot\frac{q-1}{4}}\cdot(-1)^{\frac{q-1}{4}}\left(\frac{ad-bc}{q}\right).$$

故

$$\left(\frac{q}{\pi}\right)_4\left(\frac{p}{\lambda}\right)_4=\left(\frac{\lambda}{\pi}\right)_4\left(\frac{\pi}{\lambda}\right)_4\left(\frac{\bar{\lambda}}{\pi}\right)_4\left(\frac{\bar{\pi}}{\lambda}\right)_4$$
$$=(-1)^{\frac{p-1}{4}\cdot\frac{q-1}{4}}\cdot(-1)^{\frac{p-1}{4}\cdot\frac{q-1}{4}}\cdot(-1)^{\frac{q-1}{4}}\left(\frac{ad-bc}{q}\right)=(-1)^{\frac{q-1}{4}}\left(\frac{ad-bc}{q}\right)$$

这就证明了 Burde 互反律.

由 [4] 知

$$\left(\frac{\varepsilon_p}{q}\right)=\left(\frac{q}{\pi}\right)_4\left(\frac{p}{\lambda}\right)_4=\left(\frac{\varepsilon_q}{p}\right)$$

它给出 Burde 互反律与 Scholz 互反律之间的联系.

参 考 文 献

1 K. Ireland, M. Roson, A Classical Introduction to Modern Number Theory, Springer-Verlag, New York, 1982.

2 K. Burde, Ein rationales biquadratisches Reziprozitätsgesetz, J. Reine Angew. Math., 235(1969), 175–184.

3 A. Scholz, Über die Lösbarkeit der Gleichung $t^2-Du^2=-4$, Math. Z., 39(1934),95–111.

4 E. Lehmer, Rational reciprocity laws, Amer. Math. Monthly 85 (1978), no.6, 467–472.