J. Nanjing Univ. Math. Biquarterly 9(1992), no.1, 92-101
List of the results in the paper

NOTES ON QUARTIC RESIDUE SYMBOLS AND RATIONAL RECIPROCITY LAWS

Zhi-Hong Sun

Department of Mathematics, Huaiyin Teachers College,
Huaian, Jiangsu 223001, P.R. China
E-mail: hyzhsun@public.hy.js.cn

Notations.

$\mathbb{Z}$—the set of integers, $\left(\frac{a}{m}\right)$—the Jacobi symbol, $\left(\frac{a+bi}{c+di}\right)_4$—the quartic Jacobi symbol, (m,n)—the greatest common divisor of m and n, $\mathbb{Z}[i]$—the set $\{a+bi \mid a,b\in\mathbb{Z}\}$, $\bar{\pi}$—the complex conjugate of π.

For $a,b\in\mathbb{Z}$ the Lucas sequence $\{u_n(a,b)\}$ is defined by

$$u_0(a,b)=0,\ u_1(a,b)=1 \text{ and } u_{n+1}(a,b)=bu_n(a,b)-au_{n-1}(a,b)\ (n\ge 1).$$

For odd prime p and quadratic residue $t \pmod p$ let $\sqrt{t}$ denote one of the solutions of the congruence $x^2\equiv t \pmod p$.

Proposition 1. *Let m be a positive odd number, $a,b\in\mathbb{Z}$ and $(a^2+b^2,m)=1$. Then*

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

Theorem 1. *Let p be an odd prime and $b,c\in\mathbb{Z}$.*

(1) *If $\left(\frac{b^2-c^2}{p}\right)=1$ and $p\nmid c(b+c)$, then*

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

(2) *If $p\equiv 3 \pmod 4$, $p\nmid c$ and $\left(\frac{b^2+c^2}{p}\right)=1$, then*

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

(3) *If $p\equiv 3 \pmod 4$ and $\left(\frac{b^2+c^2}{p}\right)=-1$, then*

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

Theorem 2. *Let p and q be primes such that $p \equiv 3 \pmod 4$, $q \equiv 1 \pmod 4$ and $\left(\frac{p}{q}\right) = 1$, and let $q = b^2 + c^2$ with $b, c \in \mathbb{Z}$ and $2 \mid c$.*

(i) If $p \mid c$, then $x^4 \equiv p \pmod q$ is solvable if and only if $q \equiv 1 \pmod 8$.

(ii) If $p \mid b$, then $x^4 \equiv p \pmod q$ is solvable if and only if $q \equiv p + 2 \pmod 8$.

(iii) If $p \nmid bc$, then $x^4 \equiv p \pmod q$ is solvable if and only if $\left(\frac{b+\sqrt{q}}{p}\right) = (-1)^{\frac{q-1}{4}}$, where $\sqrt{q}$ satisfies the condition $\left(\frac{\sqrt{q}}{p}\right) = (-1)^{\frac{p+1}{4}}$.

If p is a prime of the form $4k+3$, $a, b \in \mathbb{Z}$ and $\left(\frac{a^2+b^2}{p}\right) = 1$, then

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

Thus there is a unique $r \in \{0, 1, 2, 3\}$ such that $(a+bi)^{\frac{p^2-1}{8}} \equiv i^r \pmod p$. From this we define the octic residue symbol $\left(\frac{a+bi}{p}\right)_8 = i^r$.

Lemma 1. *Let p be a prime of the form $4k+3$, $a, b \in \mathbb{Z}$, $2 \nmid a$, $2 \mid b$, $\left(\frac{a^2+b^2}{p}\right) = 1$ and $\left(\frac{\sqrt{a^2+b^2}}{p}\right) = \left(\frac{a+bi}{p}\right)_4$. Then*

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

where

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

Theorem 3. *Let p be a prime of the form $4k+3$, $a, b \in \mathbb{Z}$, $p \nmid ab$, $\left(\frac{a+bi}{p}\right)_4 = 1$. Then*

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

where

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

Proposition 2. *Let $a, b, c, d \in \mathbb{Z}$, $2 \nmid c$, $2 \mid d$, $(c, d) = 1$ and $(a^2+b^2, c^2+d^2) = 1$. Then*

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

§3. The simple proofs of Burde's reciprocity law and Scholz's reciprocity law.

Let p and q be distinct primes of the form $4k+1$, and let $\varepsilon_p = (t_p + u_p\sqrt{p})/2$ and $\varepsilon_q = (t_q + u_q\sqrt{q})/2$ be the fundamental units of quadratic fields $\mathbb{Q}(\sqrt{p})$ and $\mathbb{Q}(\sqrt{q})$ respectively. Then clearly $t_p^2 - pu_p^2 = -4$ and $t_q^2 - qu_q^2 = -4$.

Scholz's reciprocity law asserts that if $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right) = 1$, then

$$\Big(\frac{\varepsilon_p}{q}\Big) = \Big(\frac{\varepsilon_q}{p}\Big).$$

Now we deduce Scholz's reciprocity law from quadratic reciprocity law. Suppose $t_p + t_q = 2^\alpha m$ with $2 \nmid m$. Then

$$\begin{aligned}\Big(\frac{m}{q}\Big) &= \Big(\frac{q}{|m|}\Big) = \Big(\frac{qu_q^2}{|m|}\Big) = \Big(\frac{pu_p^2 + t_q^2 - t_p^2}{|m|}\Big) \\ &= \Big(\frac{pu_p^2}{|m|}\Big) = \Big(\frac{p}{|m|}\Big) = \Big(\frac{m}{p}\Big).\end{aligned}$$

Thus, if $p \equiv q \pmod 8$, then $\left(\frac{2}{p}\right) = \left(\frac{2}{q}\right)$ and so

$$\Big(\frac{t_p + t_q}{p}\Big) = \Big(\frac{2^\alpha}{p}\Big)\Big(\frac{m}{p}\Big) = \Big(\frac{2^\alpha}{q}\Big)\Big(\frac{m}{q}\Big) = \Big(\frac{t_p + t_q}{q}\Big).$$

If $p \equiv 1 \pmod 8$ and $q \equiv 5 \pmod 8$, then clearly $8 \mid t_p$, $t_q \equiv 1 \pmod 2$ or $t_q \equiv 4 \pmod 8$. Hence $\alpha = 0$ or 2 and so

$$\Big(\frac{t_p + t_q}{p}\Big) = \Big(\frac{m}{p}\Big) = \Big(\frac{m}{q}\Big) = \Big(\frac{2^\alpha}{q}\Big)\Big(\frac{m}{q}\Big) = \Big(\frac{t_p + t_q}{q}\Big).$$

By symmetry, if $p \equiv 5 \pmod 8$ and $q \equiv 1 \pmod 8$, we also have $\left(\frac{t_p+t_q}{p}\right) = \left(\frac{t_p+t_q}{q}\right)$.

Now, by Theorem 1(1) we have

$$\begin{aligned}\Big(\frac{\varepsilon_p}{q}\Big) &= \Big(\frac{(t_p + u_p\sqrt{p})/2}{q}\Big) = \Big(\frac{2}{q}\Big)\Big(\frac{t_p + \sqrt{pu_p^2}}{q}\Big) = \Big(\frac{2}{q}\Big)\Big(\frac{t_p + \sqrt{t_p^2 + 4}}{q}\Big) \\ &= \Big(\frac{t_p + \sqrt{-4}}{q}\Big) = \Big(\frac{t_p + t_q}{q}\Big).\end{aligned}$$

By symmetry we also have

$$\Big(\frac{\varepsilon_q}{p}\Big) = \Big(\frac{t_p + t_q}{p}\Big).$$

Hence by the previous claim we get

$$\Big(\frac{\varepsilon_p}{q}\Big) = \Big(\frac{t_p + t_q}{q}\Big) = \Big(\frac{t_p + t_q}{p}\Big) = \Big(\frac{\varepsilon_q}{p}\Big).$$

This proves Scholz's reciprocity law.

Let p and q be distinct primes of the form $4k+1$, $p = \pi\bar{\pi}$ and $q = \lambda\bar{\lambda}$, where π and λ are primary primes in $\mathbb{Z}[i]$. Burde's reciprocity law states that if $p = a^2 + b^2,\ q = c^2 + d^2, 2 \nmid ac$ and $\left(\frac{p}{q}\right) = 1$, then

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

Now we use quartic reciprocity law to prove Burde's reciprocity law. Write $\pi = a + bi$ and $\lambda = c + di$. By Propositions 1, 2 and quartic reciprocity law we have

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

and

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

Thus

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

This proves Burde's reciprocity law.