

On the quartic character of quadratic units

by

ZHI-HONG SUN (Huaian)

1. Introduction. Let \mathbb{Z} be the set of integers and $i = \sqrt{-1}$. For any odd prime p and $a \in \mathbb{Z}$ let $\left(\frac{a}{p}\right)$ be the Legendre symbol. For $a, b, c, d \in \mathbb{Z}$ with $2 \nmid c$ and $2 \mid d$, one can define the quartic Jacobi symbol $\left(\frac{a+bi}{c+di}\right)_4$ as in [S4]. From [IR] we know that $\overline{\left(\frac{a+bi}{c+di}\right)_4} = \left(\frac{a-bi}{c-di}\right)_4 = \left(\frac{a+bi}{c+di}\right)_4^{-1}$, where \bar{x} means the complex conjugate of x . For the properties of the quartic Jacobi symbol, see [IR], [BEW], [S2] and [S4]. In particular, for $a, b \in \mathbb{Z}$ with $2 \nmid a$ and $2 \mid b$,

$$(1.1) \quad \left(\frac{i}{a+bi}\right)_4 = (-1)^{\frac{a^2-1}{8}} i^{(1-(-1)^{\frac{b}{2}})/2} \quad \text{and} \quad \left(\frac{-1}{a+bi}\right)_4 = (-1)^{\frac{b}{2}}.$$

Let $D > 1$ be a squarefree integer, and $\varepsilon_D = (m + n\sqrt{D})/2$ be the fundamental unit of the quadratic field $\mathbb{Q}(\sqrt{D})$ (where \mathbb{Q} is the set of rational numbers). Suppose that $p \equiv 1 \pmod{4}$ is a prime such that $\left(\frac{D}{p}\right) = 1$. As $\frac{m+n\sqrt{D}}{2} \cdot \frac{m-n\sqrt{D}}{2} = \frac{m^2-Dn^2}{4} = \pm 1$, we may introduce the Legendre symbol $\left(\frac{\varepsilon_D}{p}\right)$. When the norm $N(\varepsilon_D) = (m^2 - Dn^2)/4$ equals -1 , many mathematicians tried to characterize those primes p for which ε_D is a quadratic residue modulo p (that is, $\left(\frac{\varepsilon_D}{p}\right) = 1$); see [Lem]. This general problem was finally solved by the author in [S2, S3]. The next natural problem is to determine whether ε_D is a quartic residue modulo p when $\left(\frac{\varepsilon_D}{p}\right) = 1$. When the norm $N(\varepsilon_D) = (m^2 - Dn^2)/4$ equals 1 , the problem was solved by the author in [S2]. Now we assume $N(\varepsilon_D) = (m^2 - Dn^2)/4 = -1$. Using the cyclotomic numbers of order 4, in 1974 E. Lehmer [L] proved that for a prime $p = 8k + 1 = x^2 + 2y^2$ with $x, y \in \mathbb{Z}$, $\varepsilon_2 = 1 + \sqrt{2}$ is a quartic residue of p if and only if $4 \mid y$ and $\frac{p-1}{8} \equiv \frac{y}{4} \pmod{2}$. See also [S4, Corollary 3.1]. If $p \neq 17$ is a prime of the form $8k + 1$ and so $p = C^2 + 2D^2$ for some $C, D \in \mathbb{Z}$, in

2010 *Mathematics Subject Classification*: Primary 11A15; Secondary 11A07, 11B39, 11E25.

Key words and phrases: congruence, quartic residue, Lucas sequence.

[S5, Corollary 3.1] the author showed that $\varepsilon_{17} = 4 + \sqrt{17}$ is a quartic residue modulo p if and only if $p = x^2 + 17y^2$ ($x, y \in \mathbb{Z}$) and $(-1)^y = \left(\frac{2C-3D}{17}\right)$.

Let $p \equiv 1 \pmod{4}$ be a prime, $b \in \mathbb{Z}$, $2 \nmid b$, $p \neq b^2 + 4$ and $p = c^2 + d^2 = x^2 + (b^2 + 4)y^2$ for some $c, d, x, y \in \mathbb{Z}$. Suppose $c \equiv 1 \pmod{4}$, $d = 2^r d_0$ and $d_0 \equiv 1 \pmod{4}$. If $4 \mid xy$, in [S4, Conjecture 9.5] the author conjectured that

$$(1.2) \quad \varepsilon_{b^2+4}^{\frac{p-1}{4}} = \left(\frac{b + \sqrt{b^2 + 4}}{2}\right)^{\frac{p-1}{4}} \equiv \begin{cases} (-1)^{\lfloor \frac{b}{4} \rfloor + \frac{x}{4}} \frac{c}{d} \pmod{p} & \text{if } 4 \mid x, \\ (-1)^{\frac{d+y}{4}} \pmod{p} & \text{if } 4 \mid y, \end{cases}$$

where $\lfloor \cdot \rfloor$ is the greatest integer function. For $m, n \in \mathbb{Z}$ let (m, n) be the greatest common divisor of m and n . For $m \in \mathbb{Z}$ with $m = 2^\alpha m_0$ ($2 \nmid m_0$) we write $2^\alpha \parallel m$. In the paper we use the results from [S4, S6] to prove (1.2) under the condition that $(c, x + d) = 1$ or $(d_0, x + c) = 1$. More generally, we determine $\left(\frac{b + \sqrt{b^2 + 4^\alpha}}{2}\right)^{\frac{p-1}{4}} \pmod{p}$ for $p = c^2 + d^2 = x^2 + (b^2 + 4^\alpha)y^2$ ($2 \nmid b$), see Theorem 2.2. We also determine $(2a + \sqrt{4a^2 + 1})^{\frac{p-1}{4}} \pmod{p}$ for $p = c^2 + d^2 = x^2 + (4a^2 + 1)y^2$ ($a \in \mathbb{Z}$), see Corollary 4.1.

For $b, c \in \mathbb{Z}$ the *Lucas sequences* $\{U_n(b, c)\}$ and $\{V_n(b, c)\}$ are defined by

$$(1.3) \quad \begin{aligned} U_0(b, c) &= 0, & U_1(b, c) &= 1, \\ U_{n+1}(b, c) &= bU_n(b, c) - cU_{n-1}(b, c) \quad (n \geq 1) \end{aligned}$$

and

$$(1.4) \quad \begin{aligned} V_0(b, c) &= 2, & V_1(b, c) &= b, \\ V_{n+1}(b, c) &= bV_n(b, c) - cV_{n-1}(b, c) \quad (n \geq 1). \end{aligned}$$

Let $p \equiv 1 \pmod{4}$ be a prime, $b \in \mathbb{Z}$, $2 \nmid b$ and $p = c^2 + d^2 = x^2 + (b^2 + 4)y^2 \neq b^2 + 4$ for some $c, d, x, y \in \mathbb{Z}$. Suppose $c \equiv 1 \pmod{4}$, $d = 2^r d_0$, $y = 2^t y_0$ and $d_0 \equiv y_0 \equiv 1 \pmod{4}$. In [S4, Conjecture 9.4] the author conjectured that for $4 \nmid xy$,

$$U_{\frac{p-1}{4}}(b, -1) \equiv \begin{cases} (-1)^{\lfloor \frac{b}{4} \rfloor + \frac{d}{4} + \frac{x-2}{4}} \frac{2y}{x} \pmod{p} & \text{if } 2 \parallel x, \\ (-1)^{\frac{x-1}{2}} \frac{2dy}{cx} \pmod{p} & \text{if } 2 \parallel y, \end{cases}$$

and that for $4 \mid xy$,

$$V_{\frac{p-1}{4}}(b, -1) \equiv \begin{cases} -2(-1)^{\lfloor \frac{b}{4} \rfloor + \frac{x}{4}} \frac{d}{c} \pmod{p} & \text{if } 4 \mid x, \\ 2(-1)^{\frac{d+y}{4}} \pmod{p} & \text{if } 4 \mid y. \end{cases}$$

In the present paper we prove the above conjecture under the condition that $(c, x + d) = 1$ or $(d_0, x + c) = 1$. We also establish similar results for $U_{\frac{p-1}{4}}(b, -1) \pmod{p}$ and $V_{\frac{p-1}{4}}(b, -1) \pmod{p}$ in the case $b \equiv 0 \pmod{4}$. As a consequence, we obtain a criterion for $p \mid U_{\frac{p-1}{8}}(b, -1)$, where $b \in \mathbb{Z}$, $b \not\equiv 2 \pmod{4}$ and p is a prime of the form $8k + 1$, see Theorems 3.2, 3.4 and 4.2.

2. Congruences for $\left(\frac{b+\sqrt{b^2+4\alpha}}{2}\right)^{\frac{p-1}{4}} \pmod{p}$

LEMMA 2.1 ([S4, Corollary 6.1]). *Let $p \equiv 1 \pmod{4}$ be a prime and $p = c^2 + d^2$ with $c, d \in \mathbb{Z}$ and $c \equiv 1 \pmod{4}$. Let $b \in \mathbb{Z}$, $2 \nmid b$ and $p = x^2 + (b^2 + 4)y^2$ with $x, y \in \mathbb{Z}$, $x = 2^s x_0$, $y = 2^t y_0$ and $x_0 \equiv y_0 \equiv 1 \pmod{4}$. Then*

$$\left(\frac{b - \frac{cx}{dy}}{2}\right)^{\frac{p-1}{4}} \equiv \begin{cases} \mp(-1)^{\frac{b-1}{2}}(b^2+4)^{\frac{p-5}{8}}\frac{x}{y} \pmod{p} & \text{if } 2 \parallel y \text{ and } \left(\frac{2c+bd}{b+2i}\right)_4 = \pm 1, \\ \mp(-1)^{\frac{b-1}{2}}(b^2+4)^{\frac{p-5}{8}}\frac{dx}{cy} \pmod{p} & \text{if } 2 \parallel y \text{ and } \left(\frac{2c+bd}{b+2i}\right)_4 = \pm i, \\ \mp(-1)^{\frac{b-1}{2}}(b^2+4)^{\frac{p-1}{8}}\frac{d}{c} \pmod{p} & \text{if } 4 \mid y \text{ and } \left(\frac{2c+bd}{b+2i}\right)_4 = \pm 1, \\ \pm(-1)^{\frac{b-1}{2}}(b^2+4)^{\frac{p-1}{8}} \pmod{p} & \text{if } 4 \mid y \text{ and } \left(\frac{2c+bd}{b+2i}\right)_4 = \pm i, \\ \mp(-1)^{\frac{b^2-1}{8}}(b^2+4)^{\frac{p-1}{8}} \pmod{p} & \text{if } 2 \parallel x \text{ and } \left(\frac{2c+bd}{b+2i}\right)_4 = \pm 1, \\ \mp(-1)^{\frac{b^2-1}{8}}(b^2+4)^{\frac{p-1}{8}}\frac{d}{c} \pmod{p} & \text{if } 2 \parallel x \text{ and } \left(\frac{2c+bd}{b+2i}\right)_4 = \pm i, \\ \pm(-1)^{\frac{b^2-1}{8}}(b^2+4)^{\frac{p-5}{8}}\frac{dx}{cy} \pmod{p} & \text{if } 4 \mid x \text{ and } \left(\frac{2c+bd}{b+2i}\right)_4 = \pm 1, \\ \mp(-1)^{\frac{b^2-1}{8}}(b^2+4)^{\frac{p-5}{8}}\frac{x}{y} \pmod{p} & \text{if } 4 \mid x \text{ and } \left(\frac{2c+bd}{b+2i}\right)_4 = \pm i. \end{cases}$$

LEMMA 2.2 ([S6, Theorem 4.5]). *Let $p \equiv 1 \pmod{4}$ be a prime, $p = c^2 + d^2 = x^2 + (a^2 + b^2)y^2 \neq a^2 + b^2$, $a, b, c, d, x, y \in \mathbb{Z}$, $a \neq 0$, $2 \mid a$, $(a, b) = 1$, $c \equiv 1 \pmod{4}$, $d = 2^r d_0$, $y = 2^t y_0$ and $d_0 \equiv y_0 \equiv 1 \pmod{4}$. Assume $(c, x + d) = 1$ or $(d_0, x + c) = 1$. Suppose $\left(\frac{ac+bd}{b+ai}\right)_4 = i^m$.*

(i) *If $p \equiv 1 \pmod{8}$, then*

$$(a^2 + b^2)^{\frac{p-1}{8}} \equiv \begin{cases} (-1)^{\frac{d}{4} + \frac{x}{4}} \left(\frac{c}{d}\right)^m \pmod{p} & \text{if } 4 \mid a \text{ and } 2 \mid x, \\ (-1)^{\frac{d}{4} + \frac{y}{4}} \left(\frac{c}{d}\right)^m \pmod{p} & \text{if } 4 \mid a \text{ and } 2 \nmid x, \\ (-1)^{\frac{b+1}{2} + \frac{d}{4} + \frac{x-2}{4}} \left(\frac{c}{d}\right)^{m-1} \pmod{p} & \text{if } 2 \parallel a \text{ and } 2 \mid x, \\ (-1)^{\frac{b-1}{2} + \frac{d}{4} + \frac{y}{4} + \frac{x-1}{2}} \left(\frac{c}{d}\right)^{m-1} \pmod{p} & \text{if } 2 \parallel a \text{ and } 2 \nmid x. \end{cases}$$

(ii) *If $p \equiv 5 \pmod{8}$, then*

$$(a^2 + b^2)^{\frac{p-5}{8}} \equiv \begin{cases} (-1)^{\frac{x-2}{4}} \left(\frac{c}{d}\right)^{m-1} \frac{y}{x} \pmod{p} & \text{if } 4 \mid a \text{ and } 2 \mid x, \\ (-1)^{\frac{x+1}{2}} \left(\frac{c}{d}\right)^{m-1} \frac{y}{x} \pmod{p} & \text{if } 4 \mid a \text{ and } 2 \nmid x, \\ (-1)^{\frac{x}{4} + \frac{b+1}{2}} \left(\frac{c}{d}\right)^m \frac{y}{x} \pmod{p} & \text{if } 2 \parallel a \text{ and } 2 \mid x, \\ (-1)^{\frac{b-1}{2}} \left(\frac{c}{d}\right)^m \frac{y}{x} \pmod{p} & \text{if } 2 \parallel a \text{ and } 2 \nmid x. \end{cases}$$

THEOREM 2.1. *Let $p \equiv 1 \pmod{4}$ be a prime, $b \in \mathbb{Z}$, $2 \nmid b$, $p \neq b^2 + 4$ and $p = c^2 + d^2 = x^2 + (b^2 + 4)y^2$ for some $c, d, x, y \in \mathbb{Z}$. Suppose $c \equiv 1 \pmod{4}$, $d = 2^r d_0$, $x = 2^s x_0 (2 \nmid x_0)$, $y = 2^t y_0$ and $d_0 \equiv y_0 \equiv 1 \pmod{4}$. Assume $(c, x + d) = 1$ or $(d_0, x + c) = 1$.*

(i) If $4 \nmid xy$, then

$$\begin{aligned} \left(\frac{b + (-1)^{\frac{x_0-1}{2}} \frac{cx}{dy}}{2} \right)^{\frac{p-1}{4}} &\equiv - \left(\frac{b - (-1)^{\frac{x_0-1}{2}} \frac{cx}{dy}}{2} \right)^{\frac{p-1}{4}} \\ &\equiv \begin{cases} (-1)^{\lfloor \frac{b}{4} \rfloor + \frac{d}{4}} \frac{c}{d} \pmod{p} & \text{if } 2 \parallel x, \\ 1 \pmod{p} & \text{if } 2 \parallel y. \end{cases} \end{aligned}$$

(ii) If $4 \mid xy$, then

$$\left(\frac{b + \frac{cx}{dy}}{2} \right)^{\frac{p-1}{4}} \equiv \left(\frac{b - \frac{cx}{dy}}{2} \right)^{\frac{p-1}{4}} \equiv \begin{cases} (-1)^{\lfloor \frac{b}{4} \rfloor + \frac{x}{4}} \frac{c}{d} \pmod{p} & \text{if } 4 \mid x, \\ (-1)^{\frac{d}{4} + \frac{y}{4}} \pmod{p} & \text{if } 4 \mid y. \end{cases}$$

Proof. Since $\left(\frac{-1}{b+2i}\right)_4 = -1$ by (1.1), replacing x with $(-1)^{(x_0-1)/2}x$ in Lemma 2.1 we get

$$(2.1) \quad \left(\frac{b - (-1)^{\frac{x_0-1}{2}} \frac{cx}{dy}}{2} \right)^{\frac{p-1}{4}} \equiv \begin{cases} \mp (-1)^{\frac{b-1}{2}} (b^2 + 4)^{\frac{p-5}{8}} \frac{x}{y} \pmod{p} & \text{if } 2 \parallel y \text{ and } \left(\frac{2c+bd}{b+2i}\right)_4 = \pm 1, \\ \mp (-1)^{\frac{b-1}{2}} (b^2 + 4)^{\frac{p-5}{8}} \frac{dx}{cy} \pmod{p} & \text{if } 2 \parallel y \text{ and } \left(\frac{2c+bd}{b+2i}\right)_4 = \pm i, \\ \mp (-1)^{\frac{b-1}{2} + \frac{x_0-1}{2}} (b^2 + 4)^{\frac{p-1}{8}} \frac{d}{c} \pmod{p} & \text{if } 4 \mid y \text{ and } \left(\frac{2c+bd}{b+2i}\right)_4 = \pm 1, \\ \pm (-1)^{\frac{b-1}{2} + \frac{x_0-1}{2}} (b^2 + 4)^{\frac{p-1}{8}} \pmod{p} & \text{if } 4 \mid y \text{ and } \left(\frac{2c+bd}{b+2i}\right)_4 = \pm i, \\ \mp (-1)^{\frac{b^2-1}{8} + \frac{x_0-1}{2}} (b^2 + 4)^{\frac{p-1}{8}} \pmod{p} & \text{if } 2 \parallel x \text{ and } \left(\frac{2c+bd}{b+2i}\right)_4 = \pm 1, \\ \mp (-1)^{\frac{b^2-1}{8} + \frac{x_0-1}{2}} (b^2 + 4)^{\frac{p-1}{8}} \frac{d}{c} \pmod{p} & \text{if } 2 \parallel x \text{ and } \left(\frac{2c+bd}{b+2i}\right)_4 = \pm i, \\ \pm (-1)^{\frac{b^2-1}{8}} (b^2 + 4)^{\frac{p-5}{8}} \frac{dx}{cy} \pmod{p} & \text{if } 4 \mid x \text{ and } \left(\frac{2c+bd}{b+2i}\right)_4 = \pm 1, \\ \mp (-1)^{\frac{b^2-1}{8}} (b^2 + 4)^{\frac{p-5}{8}} \frac{x}{y} \pmod{p} & \text{if } 4 \mid x \text{ and } \left(\frac{2c+bd}{b+2i}\right)_4 = \pm i. \end{cases}$$

Taking $a = 2$ in Lemma 2.2 we obtain

$$(b^2 + 4)^{\lfloor \frac{p}{8} \rfloor} \equiv \begin{cases} (-1)^{\frac{b+1}{2} + \frac{d}{4} + \frac{x_0-1}{2}} \left(\frac{c}{d}\right)^{m-1} \pmod{p} & \text{if } 2 \parallel x, \\ (-1)^{\frac{b-1}{2}} \left(\frac{c}{d}\right)^m \frac{y}{x} \pmod{p} & \text{if } 2 \parallel y, \\ (-1)^{\frac{x}{4} + \frac{b+1}{2}} \left(\frac{c}{d}\right)^m \frac{y}{x} \pmod{p} & \text{if } 4 \mid x, \\ (-1)^{\frac{b-1}{2} + \frac{d}{4} + \frac{y}{4} + \frac{x_0-1}{2}} \left(\frac{c}{d}\right)^{m-1} \pmod{p} & \text{if } 4 \mid y. \end{cases}$$

This together with (2.1) yields

$$(2.2) \quad \left(\frac{b - (-1)^{\frac{x_0-1}{2}} \frac{cx}{dy}}{2} \right)^{\frac{p-1}{4}} \equiv \begin{cases} -(-1)^{\lfloor \frac{b}{4} \rfloor + \frac{d}{4}} \frac{c}{d} \pmod{p} & \text{if } 2 \parallel x, \\ -1 \pmod{p} & \text{if } 2 \parallel y, \\ (-1)^{\lfloor \frac{b}{4} \rfloor + \frac{x}{4}} \frac{c}{d} \pmod{p} & \text{if } 4 \mid x, \\ (-1)^{\frac{d}{4} + \frac{y}{4}} \pmod{p} & \text{if } 4 \mid y. \end{cases}$$

Since

$$\frac{b + (-1)^{\frac{x_0-1}{2}} \frac{cx}{dy}}{2} \cdot \frac{b - (-1)^{\frac{x_0-1}{2}} \frac{cx}{dy}}{2} \equiv \frac{b^2 - (b^2 + 4)}{4} = -1 \pmod{p},$$

we see that

$$(2.3) \quad \left(\frac{b + (-1)^{\frac{x_0-1}{2}} \frac{cx}{dy}}{2} \right)^{\frac{p-1}{4}} \equiv (-1)^{\frac{p-1}{4}} \left(\frac{b - (-1)^{\frac{x_0-1}{2}} \frac{cx}{dy}}{2} \right)^{-\frac{p-1}{4}} \pmod{p}.$$

Now combining (2.2) with (2.3) we deduce the result.

COROLLARY 2.1. *Let $p \equiv 1 \pmod{4}$ be a prime, $b \in \mathbb{Z}$, $2 \nmid b$, $p \neq b^2 + 4$ and $p = c^2 + d^2 = x^2 + (b^2 + 4)y^2$ with $c, d, x, y \in \mathbb{Z}$ and $4 \mid xy$. Suppose $c \equiv 1 \pmod{4}$, $d = 2^r d_0$ and $d_0 \equiv 1 \pmod{4}$. Assume $(c, x + d) = 1$ or $(d_0, x + c) = 1$. Then*

$$\left(\frac{b + \sqrt{b^2 + 4}}{2} \right)^{\frac{p-1}{4}} \equiv \begin{cases} (-1)^{\lfloor \frac{b}{4} \rfloor + \frac{x}{4}} \frac{c}{d} \pmod{p} & \text{if } 4 \mid x, \\ (-1)^{\frac{d}{4} + \frac{y}{4}} \pmod{p} & \text{if } 4 \mid y. \end{cases}$$

THEOREM 2.2. *Let $p \equiv 1 \pmod{4}$ be a prime, $\alpha \in \{2, 3, 4, \dots\}$, $b \in \mathbb{Z}$, $2 \nmid b$, $p \neq b^2 + 4^\alpha$ and $p = c^2 + d^2 = x^2 + (b^2 + 4^\alpha)y^2$ for some $c, d, x, y \in \mathbb{Z}$. Suppose $c \equiv 1 \pmod{4}$, $d = 2^r d_0$, $x = 2^s x_0 (2 \nmid x_0)$, $y = 2^t y_0$ and $d_0 \equiv y_0 \equiv 1 \pmod{4}$. Assume $(c, x + d) = 1$ or $(d_0, x + c) = 1$.*

(i) *If $p \equiv 1 \pmod{8}$, then*

$$\left(\frac{b - \frac{cx}{dy}}{2} \right)^{\frac{p-1}{4}} \equiv \left(\frac{b + \frac{cx}{dy}}{2} \right)^{\frac{p-1}{4}} \equiv \begin{cases} (-1)^{\frac{b^2-1}{8} + 2^{\alpha-2} + \frac{d+x}{4}} \alpha \pmod{p} & \text{if } 4 \mid x, \\ (-1)^{\frac{d+y}{4}} \alpha \pmod{p} & \text{if } 4 \mid y. \end{cases}$$

(ii) *If $p \equiv 5 \pmod{8}$, then*

$$\begin{aligned} \left(\frac{b - (-1)^{\frac{x_0-1}{2}} \frac{cx}{dy}}{2} \right)^{\frac{p-1}{4}} &\equiv (-1)^\alpha \left(\frac{b + (-1)^{\frac{x_0-1}{2}} \frac{cx}{dy}}{2} \right)^{\frac{p-1}{4}} \\ &\equiv \begin{cases} (-1)^{\frac{(b+2)^2-9}{8} + \frac{b+1}{2} \alpha + 2^{\alpha-2}} \pmod{p} & \text{if } 2 \parallel x, \\ (-1)^{\frac{b-1}{2}(\alpha+1)} \pmod{p} & \text{if } 2 \parallel y. \end{cases} \end{aligned}$$

Proof. It is clear that

$$(2.4) \quad \begin{aligned} &\left(\frac{b + \frac{cx}{dy}}{2} \right)^{\frac{p-1}{4}} \left(\frac{b - \frac{cx}{dy}}{2} \right)^{\frac{p-1}{4}} \\ &\equiv \left(\frac{b^2 - (b^2 + 4^\alpha)}{4} \right)^{\frac{p-1}{4}} = (-1)^{\frac{p-1}{4}} 2^{\frac{p-1}{2}(\alpha-1)} \equiv (-1)^{\frac{p-1}{4}} \alpha \pmod{p}. \end{aligned}$$

By [IR, p. 64] we have

$$(2.5) \quad 2^{\frac{p-1}{4}} \equiv \left(\frac{d}{c} \right)^{\frac{cd}{2}} \equiv \left(\frac{d}{c} \right)^{\frac{d}{2}} \equiv \begin{cases} (-1)^{\frac{d}{4}} \pmod{p} & \text{if } p \equiv 1 \pmod{8}, \\ \frac{d}{c} \pmod{p} & \text{if } p \equiv 5 \pmod{8}. \end{cases}$$

Suppose that $\left(\frac{(2^\alpha c + bd)/x}{b + 2^\alpha i}\right)_4 = i^m$. As $\left(\frac{-1}{b + 2^\alpha i}\right)_4 = 1$ we have $\left(\frac{(2^\alpha c + bd)/(-x)}{b + 2^\alpha i}\right)_4 = i^m$. By [S4, Theorem 6.1], (2.5) and Lemma 2.2 we have the following conclusions: If $p \equiv 1 \pmod{8}$ and $4 \mid x$, then

$$\begin{aligned} & \left(\frac{b - (-1)^{\frac{x_0-1}{2}} \frac{cx}{dy}}{2}\right)^{\frac{p-1}{4}} \\ & \equiv (-1)^{\frac{b^2-1}{8} + (\alpha+1)\frac{2^\alpha - (-1)^{(x_0-1)/2}x}{4} + (\alpha-1)\frac{d}{4}} \left(\frac{d}{c}\right)^m (2^{2\alpha} + b^2)^{\frac{p-1}{8}} \\ & \equiv (-1)^{\frac{b^2-1}{8} + (\alpha+1)\frac{2^\alpha - (-1)^{(x_0-1)/2}x}{4} + (\alpha-1)\frac{d}{4}} \left(\frac{d}{c}\right)^m \cdot (-1)^{\frac{d}{4} + \frac{x}{4}} \left(\frac{c}{d}\right)^m \\ & = (-1)^{\frac{b^2-1}{8} + 2^{\alpha-2}(\alpha+1) + \frac{d}{4}\alpha + \frac{x}{4}\alpha} = (-1)^{\frac{b^2-1}{8} + 2^{\alpha-2} + \frac{d+x}{4}\alpha} \pmod{p}. \end{aligned}$$

If $p \equiv 1 \pmod{8}$ and $4 \mid y$, then

$$\begin{aligned} & \left(\frac{b - (-1)^{\frac{x_0-1}{2}} \frac{cx}{dy}}{2}\right)^{\frac{p-1}{4}} \equiv (-1)^{(\alpha+1)\frac{y}{4} + (\alpha-1)\frac{d}{4}} \left(\frac{d}{c}\right)^m (2^{2\alpha} + b^2)^{\frac{p-1}{8}} \\ & \equiv (-1)^{(\alpha+1)\frac{y}{4} + (\alpha-1)\frac{d}{4}} \left(\frac{d}{c}\right)^m \cdot (-1)^{\frac{d}{4} + \frac{y}{4}} \left(\frac{c}{d}\right)^m \\ & = (-1)^{\frac{d+y}{4}\alpha} \pmod{p}. \end{aligned}$$

If $p \equiv 5 \pmod{8}$ and $2 \parallel y$, then

$$\begin{aligned} & \left(\frac{b - (-1)^{\frac{x_0-1}{2}} \frac{cx}{dy}}{2}\right)^{\frac{p-1}{4}} \\ & \equiv (-1)^{\frac{b+1}{2}} \left(\frac{d}{c}\right)^{m-b\alpha+\alpha-1} (-1)^{\frac{x_0-1}{2}} \frac{x}{y} (2^{2\alpha} + b^2)^{\frac{p-5}{8}} \\ & \equiv (-1)^{\frac{b+1}{2}} \left(\frac{d}{c}\right)^{m-b\alpha+\alpha-1} (-1)^{\frac{x_0-1}{2}} \frac{x}{y} \cdot (-1)^{\frac{x_0-1}{2}} \left(\frac{c}{d}\right)^{m+1} \frac{y}{x} \\ & \equiv (-1)^{\frac{b-1}{2}(\alpha+1)} \pmod{p}. \end{aligned}$$

If $p \equiv 5 \pmod{8}$ and $2 \parallel x$, then

$$\begin{aligned} & \left(\frac{b - (-1)^{\frac{x_0-1}{2}} \frac{cx}{dy}}{2}\right)^{\frac{p-1}{4}} \\ & \equiv -(-1)^{\frac{(b+2)^2-9}{8} + 2^{\alpha-2}} \left(\frac{d}{c}\right)^{m+(-1)^{(b-1)/2}\alpha+\alpha-1} (-1)^{\frac{x_0-1}{2}} \frac{x}{y} (2^{2\alpha} + b^2)^{\frac{p-5}{8}} \end{aligned}$$

$$\begin{aligned} &\equiv -(-1)^{\frac{(b+2)^2-9}{8}+2\alpha-2} \left(\frac{d}{c}\right)^{m+(-1)^{(b-1)/2}\alpha+\alpha-1} (-1)^{\frac{x_0-1}{2}} \frac{x}{y} \\ &\quad \cdot (-1)^{\frac{x-2}{4}} \left(\frac{c}{d}\right)^{m-1} \frac{y}{x} \\ &\equiv (-1)^{\frac{(b+2)^2-9}{8}+\frac{b+1}{2}\alpha+2\alpha-2} \pmod{p}. \end{aligned}$$

Now putting all the above together we derive the result.

REMARK 2.1. In [S4, Theorem 5.1(iv)], the number $(-1)^{\frac{p-4a_0-b^2}{8}}$ should be $(-1)^{\frac{p-4a_0-b^2}{8}+2r-2}$. In [S4, Theorem 6.1(ii)], $(-1)^{\frac{(a_0+2)^2-(b+2)^2}{8}}$ should be $(-1)^{\frac{(a_0+2)^2-(b+2)^2}{8}+2r-2}$. In the case $2 \nmid y, 4 \mid a$ and $8 \mid p-5$ on page 518 of [S4], $(-1)^{\frac{p-4a_0-b^2}{8}+\frac{a_0^2-1}{8}}$ should be $(-1)^{\frac{p-4a_0-b^2}{8}+\frac{a_0^2-1}{8}+2r-2}$.

Taking $\alpha = 2$ in Theorem 2.2 we deduce the following result.

COROLLARY 2.2. *Let $p \equiv 1 \pmod{4}$ be a prime, $b \in \mathbb{Z}$, $2 \nmid b, p \neq b^2 + 16$ and $p = c^2 + d^2 = x^2 + (b^2 + 16)y^2$ for some $c, d, x, y \in \mathbb{Z}$. Suppose $c \equiv 1 \pmod{4}$ and $d = 2^r d_0$ with $d_0 \equiv 1 \pmod{4}$. Assume $(c, x + d) = 1$ or $(d_0, x + c) = 1$. Then*

$$\left(\frac{b + \sqrt{b^2 + 16}}{2}\right)^{\frac{p-1}{4}} \equiv \begin{cases} (-1)^y \pmod{p} & \text{if } b \equiv 1 \pmod{8}, \\ (-1)^{\frac{p-1}{4}} \pmod{p} & \text{if } b \equiv 3 \pmod{8}, \\ 1 \pmod{p} & \text{if } b \equiv 5 \pmod{8}, \\ (-1)^{\frac{p-1}{4}+y} \pmod{p} & \text{if } b \equiv 7 \pmod{8}. \end{cases}$$

REMARK 2.2. We conjecture that the condition $(c, x+d) = 1$ or $(d_0, x+c) = 1$ in Theorems 2.1–2.2 and Corollaries 2.1–2.2 can be canceled. See [S4, Conjecture 9.5].

3. Congruences for $U_{\frac{p-1}{4}}(b, -4^{\alpha-1})$ and $V_{\frac{p-1}{4}}(b, -4^{\alpha-1}) \pmod{p}$. Let $\{U_n(b, c)\}$ and $\{V_n(b, c)\}$ be the Lucas sequences given by (1.3) and (1.4). Set $d = b^2 - 4c$. It is well known that for any positive integer n ,

$$(3.1) \quad U_n(b, c) = \begin{cases} \frac{1}{\sqrt{d}} \left\{ \left(\frac{b+\sqrt{d}}{2}\right)^n - \left(\frac{b-\sqrt{d}}{2}\right)^n \right\} & \text{if } d \neq 0, \\ n \left(\frac{b}{2}\right)^{n-1} & \text{if } d = 0 \end{cases}$$

and

$$(3.2) \quad V_n(b, c) = \left(\frac{b + \sqrt{d}}{2}\right)^n + \left(\frac{b - \sqrt{d}}{2}\right)^n.$$

From [S1, Lemma 6.1(b)] we know that if $p > 3$ is a prime such that $p \nmid bcd$, then

$$(3.3) \quad p \mid U_n(b, c) \Leftrightarrow V_{2n}(b, c) \equiv 2c^n \pmod{p}.$$

THEOREM 3.1. *Let $p \equiv 1 \pmod{4}$ be a prime, $b \in \mathbb{Z}$, $2 \nmid b$ and $p = c^2 + d^2 = x^2 + (b^2 + 4)y^2 \neq b^2 + 4$ for some $c, d, x, y \in \mathbb{Z}$. Suppose $c \equiv 1 \pmod{4}$, $d = 2^r d_0$, $y = 2^t y_0$ and $d_0 \equiv y_0 \equiv 1 \pmod{4}$. Assume $(c, x + d) = 1$ or $(d_0, x + c) = 1$.*

(i) *If $4 \nmid xy$, then $V_{\frac{p-1}{4}}(b, -1) \equiv 0 \pmod{p}$ and*

$$U_{\frac{p-1}{4}}(b, -1) \equiv \begin{cases} (-1)^{\lfloor \frac{b}{4} \rfloor + \frac{d}{4} + \frac{x-2}{4} \frac{2y}{x}} \pmod{p} & \text{if } 2 \parallel x, \\ (-1)^{\frac{x-1}{2}} \frac{2dy}{cx} \pmod{p} & \text{if } 2 \parallel y. \end{cases}$$

(ii) *If $4 \mid xy$, then $U_{\frac{p-1}{4}}(b, -1) \equiv 0 \pmod{p}$ and*

$$V_{\frac{p-1}{4}}(b, -1) \equiv \begin{cases} 2(-1)^{\lfloor \frac{b}{4} \rfloor + \frac{x}{4} \frac{c}{d}} \pmod{p} & \text{if } 4 \mid x, \\ 2(-1)^{\frac{d+y}{4}} \pmod{p} & \text{if } 4 \mid y. \end{cases}$$

Proof. Suppose $x = 2^s x_0$ with $2 \nmid x_0$. Since $(\frac{cx}{dy})^2 \equiv b^2 + 4 \pmod{p}$, using (3.1) and (3.2) we see that

$$\begin{aligned} &U_{\frac{p-1}{4}}(b, -1) \\ &\equiv (-1)^{\frac{x_0-1}{2}} \frac{dy}{cx} \left\{ \left(\frac{b + (-1)^{\frac{x_0-1}{2}} \frac{cx}{dy}}{2} \right)^{\frac{p-1}{4}} - \left(\frac{b - (-1)^{\frac{x_0-1}{2}} \frac{cx}{dy}}{2} \right)^{\frac{p-1}{4}} \right\} \pmod{p} \end{aligned}$$

and

$$V_{\frac{p-1}{4}}(b, -1) \equiv \left(\frac{b + \frac{cx}{dy}}{2} \right)^{\frac{p-1}{4}} + \left(\frac{b - \frac{cx}{dy}}{2} \right)^{\frac{p-1}{4}} \pmod{p}.$$

Now applying Theorem 2.1 we deduce the result.

REMARK 3.1. When p is a prime of the form $8k+1$ and $p = c^2 + d^2 = x^2 + (b^2 + 4)y^2$ with $b \in \{1, 3\}$ and $4 \mid y$, the conjecture $V_{\frac{p-1}{4}}(b, -1) \equiv 2(-1)^{\frac{d+y}{4}} \pmod{p}$ is equivalent to a conjecture of E. Lehmer. See [L, Conjecture 4].

THEOREM 3.2. *Let $p \equiv 1 \pmod{8}$ be a prime, $b \in \mathbb{Z}$, $2 \nmid b$ and $p = c^2 + d^2 = x^2 + (b^2 + 4)y^2 \neq b^2 + 4$ for some $c, d, x, y \in \mathbb{Z}$. Suppose $c \equiv 1 \pmod{4}$ and $d = 2^r d_0$ with $d_0 \equiv 1 \pmod{4}$. Assume $(c, x + d) = 1$ or $(d_0, x + c) = 1$. Then $p \mid U_{\frac{p-1}{8}}(b, -1)$ if and only if $y \equiv \frac{p-1}{2} + d \pmod{8}$.*

Proof. This is immediate from (3.3) and Theorem 3.1.

Using (3.1), (3.2) and Theorem 2.2 one can similarly prove the following result.

THEOREM 3.3. *Let $p \equiv 1 \pmod{4}$ be a prime, $b, \alpha \in \mathbb{Z}$, $\alpha \geq 2$, $2 \nmid b$, $p \neq b^2 + 4^\alpha$ and $p = c^2 + d^2 = x^2 + (b^2 + 4^\alpha)y^2$ for some $c, d, x, y \in \mathbb{Z}$. Suppose $c \equiv 1 \pmod{4}$, $d = 2^r d_0$, $y = 2^t y_0$ and $d_0 \equiv y_0 \equiv 1 \pmod{4}$. Assume $(c, x + d) = 1$ or $(d_0, x + c) = 1$.*

(i) If $p \equiv 1 \pmod{8}$, then $U_{\frac{p-1}{4}}(b, -4^{\alpha-1}) \equiv 0 \pmod{p}$ and

$$V_{\frac{p-1}{4}}(b, -4^{\alpha-1}) \equiv \begin{cases} 2(-1)^{\frac{b^2-1}{8}+2^{\alpha-2}+\frac{d+x}{4}\alpha} \pmod{p} & \text{if } 4 \mid x, \\ 2(-1)^{\frac{d+y}{4}\alpha} \pmod{p} & \text{if } 4 \mid y. \end{cases}$$

(ii) If $p \equiv 5 \pmod{8}$, then

$$U_{\frac{p-1}{4}}(b, -4^{\alpha-1}) \equiv \begin{cases} 0 \pmod{p} & \text{if } 2 \mid \alpha, \\ 2(-1)^{\frac{(b+2)^2-1}{8}+\frac{b+1}{2}+\frac{x-2}{4}\frac{dy}{cx}} \pmod{p} & \text{if } 2 \nmid \alpha \text{ and } 2 \parallel x, \\ 2(-1)^{\frac{x+1}{2}\frac{dy}{cx}} \pmod{p} & \text{if } 2 \nmid \alpha \text{ and } 2 \parallel y \end{cases}$$

and

$$V_{\frac{p-1}{4}}(b, -4^{\alpha-1}) \equiv \begin{cases} 0 \pmod{p} & \text{if } 2 \nmid \alpha, \\ 2(-1)^{\frac{(b+2)^2-9}{8}+2^{\alpha-2}} \pmod{p} & \text{if } 2 \mid \alpha \text{ and } 2 \parallel x, \\ 2(-1)^{\frac{b-1}{2}} \pmod{p} & \text{if } 2 \mid \alpha \text{ and } 2 \parallel y. \end{cases}$$

From (2.5), (3.3) and Theorem 3.3 we derive the following result.

THEOREM 3.4. *Let $p \equiv 1 \pmod{8}$ be a prime, $b, \alpha \in \mathbb{Z}$, $\alpha \geq 2$, $2 \nmid b$, $p \neq b^2 + 4^\alpha$ and $p = c^2 + d^2 = x^2 + (b^2 + 4^\alpha)y^2$ for some $c, d, x, y \in \mathbb{Z}$. Suppose $c \equiv 1 \pmod{4}$ and $d = 2^r d_0$ with $d_0 \equiv 1 \pmod{4}$. Assume $(c, x + d) = 1$ or $(d_0, x + c) = 1$. Then*

$$p \mid U_{\frac{p-1}{8}}(b, -4^{\alpha-1}) \Leftrightarrow \frac{p-1}{8} + \frac{d}{4} \equiv \begin{cases} \frac{b^2-1}{8} + 2^{\alpha-2} + \frac{x}{4}\alpha \pmod{2} & \text{if } 4 \mid x, \\ \frac{y}{4}\alpha \pmod{2} & \text{if } 4 \mid y. \end{cases}$$

4. Congruences for $U_{\frac{p-1}{4}}(4a, -1)$ and $V_{\frac{p-1}{4}}(4a, -1) \pmod{p}$

THEOREM 4.1. *Let $a \in \mathbb{Z}$, $a \neq 0$ and let $p \equiv 1 \pmod{4}$ be a prime such that $p = c^2 + d^2 = x^2 + (4a^2 + 1)y^2$ with $c, d, x, y \in \mathbb{Z}$, $c \equiv 1 \pmod{4}$ and $p \neq 4a^2 + 1$. Suppose $d = 2^r d_0$, $y = 2^t y_0$ and $d_0 \equiv y_0 \equiv 1 \pmod{4}$. Assume that $(c, x + d) = 1$ or $(d_0, x + c) = 1$.*

(i) If $p \equiv 1 \pmod{8}$, then

$$U_{\frac{p-1}{4}}(4a, -1) \equiv \begin{cases} (-1)^{\frac{a+1}{2}+\frac{d}{4}+\frac{x-2}{4}\frac{y}{x}} \pmod{p} & \text{if } 2 \nmid ay, \\ 0 \pmod{p} & \text{if } 2 \mid ay \end{cases}$$

and

$$V_{\frac{p-1}{4}}(4a, -1) \equiv \begin{cases} 2(-1)^{\frac{d}{4}+\frac{a}{2}y+\frac{xy}{4}} \pmod{p} & \text{if } 2 \mid a, \\ 2(-1)^{\frac{d}{4}+\frac{y}{4}} \pmod{p} & \text{if } 2 \nmid a \text{ and } 2 \mid y, \\ 0 \pmod{p} & \text{if } 2 \nmid ay. \end{cases}$$

(ii) If $p \equiv 5 \pmod{8}$, then

$$U_{\frac{p-1}{4}}(4a, -1) \equiv \begin{cases} (-1)^{\frac{a}{2} + \frac{x-2}{4}} \frac{dy}{cx} \pmod{p} & \text{if } 2 \mid a \text{ and } 2 \nmid y, \\ (-1)^{\frac{x+1}{2}} \frac{dy}{cx} \pmod{p} & \text{if } 2 \mid a \text{ and } 2 \mid y, \\ (-1)^{\frac{x-1}{2}} \frac{dy}{cx} \pmod{p} & \text{if } 2 \nmid a \text{ and } 2 \mid y, \\ 0 \pmod{p} & \text{if } 2 \nmid ay \end{cases}$$

and

$$V_{\frac{p-1}{4}}(4a, -1) \equiv \begin{cases} 0 \pmod{p} & \text{if } 2 \mid ay, \\ 2(-1)^{\frac{a-1}{2} + \frac{x}{4}} \frac{d}{c} \pmod{p} & \text{if } 2 \nmid ay. \end{cases}$$

Proof. Clearly $(4a^2 + 1, x) \mid p$ and so $(4a^2 + 1, x) = 1$. As $(d - 2ac)(d + 2ac) = d^2 - 4a^2c^2 \equiv x^2 - c^2 - 4a^2c^2 \equiv x^2 \pmod{4a^2 + 1}$, we see that $(d - 2ac, 4a^2 + 1) = 1$. Suppose $(\frac{d-2ac}{1-2ai}/x)_4 = i^m$ and $x = 2^s x_0$ ($2 \nmid x_0$). Since $(\frac{-1}{1-2ai})_4 = (-1)^a$ by (1.1), replacing x with $(-1)^{(x_0-1)/2} x$ in [S4, Theorem 7.3] we see that for $p \equiv 1 \pmod{8}$,

$$U_{\frac{p-1}{4}}(4a, -1) \equiv \begin{cases} (-1)^{\frac{a+1}{2}} \frac{y}{x} \left(\frac{d}{c}\right)^{m+1} (4a^2 + 1)^{\frac{p-1}{8}} \pmod{p} & \text{if } 2 \nmid ay, \\ 0 \pmod{p} & \text{if } 2 \mid ay \end{cases}$$

and

$$V_{\frac{p-1}{4}}(4a, -1) \equiv \begin{cases} 2(-1)^{\frac{a}{2}} y \left(\frac{d}{c}\right)^m (4a^2 + 1)^{\frac{p-1}{8}} \pmod{p} & \text{if } 2 \mid a, \\ 2(-1)^{\frac{x+1}{2}} \left(\frac{d}{c}\right)^{m+1} (4a^2 + 1)^{\frac{p-1}{8}} \pmod{p} & \text{if } 2 \nmid a \text{ and } 2 \mid y, \\ 0 \pmod{p} & \text{if } 2 \nmid ay, \end{cases}$$

and that for $p \equiv 5 \pmod{8}$,

$$U_{\frac{p-1}{4}}(4a, -1) \equiv \begin{cases} (-1)^{\frac{a}{2}} y \left(\frac{d}{c}\right)^m (4a^2 + 1)^{\frac{p-5}{8}} \pmod{p} & \text{if } 2 \mid a, \\ (-1)^{\frac{x-1}{2}} \left(\frac{d}{c}\right)^{m+1} (4a^2 + 1)^{\frac{p-5}{8}} \pmod{p} & \text{if } 2 \nmid a \text{ and } 2 \mid y, \\ 0 \pmod{p} & \text{if } 2 \nmid ay \end{cases}$$

and

$$V_{\frac{p-1}{4}}(4a, -1) \equiv \begin{cases} 0 \pmod{p} & \text{if } 2 \mid ay, \\ 2(-1)^{\frac{a+1}{2}} \frac{x}{y} \left(\frac{d}{c}\right)^{m+1} (4a^2 + 1)^{\frac{p-5}{8}} \pmod{p} & \text{if } 2 \nmid ay. \end{cases}$$

Replacing a, b with $-2a, 1$ in Lemma 2.2 we see that for $p \equiv 1 \pmod{8}$,

$$(4a^2 + 1)^{\frac{p-1}{8}} \equiv \begin{cases} (-1)^{\frac{d}{4} + \frac{xy}{4}} \left(\frac{c}{d}\right)^m \pmod{p} & \text{if } 2 \mid a, \\ (-1)^{\frac{d}{4} + \frac{x+2}{4}} \left(\frac{c}{d}\right)^{m-1} \pmod{p} & \text{if } 2 \nmid ay, \\ (-1)^{\frac{d}{4} + \frac{x-1}{2} + \frac{y}{4}} \left(\frac{c}{d}\right)^{m-1} \pmod{p} & \text{if } 2 \nmid a \text{ and } 2 \mid y, \end{cases}$$

while for $p \equiv 5 \pmod{8}$,

$$(4a^2 + 1)^{\frac{p-5}{8}} \equiv \begin{cases} (-1)^{\frac{x-2}{4}} \left(\frac{c}{d}\right)^{m-1} \frac{y}{x} \pmod{p} & \text{if } 2 \mid a \text{ and } 2 \nmid y, \\ (-1)^{\frac{x+1}{2}} \left(\frac{c}{d}\right)^{m-1} \frac{y}{x} \pmod{p} & \text{if } 2 \mid a \text{ and } 2 \mid y, \\ (-1)^{\frac{x}{4}+1} \left(\frac{c}{d}\right)^m \frac{y}{x} \pmod{p} & \text{if } 2 \nmid a, \\ \left(\frac{c}{d}\right)^m \frac{y}{x} \pmod{p} & \text{if } 2 \nmid a \text{ and } 2 \mid y. \end{cases}$$

Now putting all the above together we deduce the result.

COROLLARY 4.1. *Let $a \in \mathbb{Z}$, $a \neq 0$ and let $p \equiv 1 \pmod{4}$ be a prime such that $p = c^2 + d^2 = x^2 + (4a^2 + 1)y^2$ with $c, d, x, y \in \mathbb{Z}$, $c \equiv 1 \pmod{4}$ and $p \neq 4a^2 + 1$. Suppose $d = 2^r d_0$ with $d_0 \equiv 1 \pmod{4}$. Assume that $(c, x + d) = 1$ or $(d_0, x + c) = 1$. If $4 \mid xy$, then*

$$(2a + \sqrt{4a^2 + 1})^{\frac{p-1}{4}} \equiv \begin{cases} (-1)^{\frac{d}{4} + \frac{a}{2}y + \frac{xy}{4}} \pmod{p} & \text{if } 2 \mid a, \\ (-1)^{\frac{d}{4} + \frac{y}{4}} \pmod{p} & \text{if } 2 \nmid a \text{ and } 4 \mid y, \\ (-1)^{\frac{a-1}{2} + \frac{x}{4} \frac{d}{c}} \pmod{p} & \text{if } 2 \nmid a \text{ and } 4 \mid x. \end{cases}$$

Proof. Suppose $4 \mid xy$. By Theorem 4.1, $p \mid U_{\frac{p-1}{4}}(4a, -1)$. Hence, using (3.1) and (3.2) we see that

$$\begin{aligned} (2a + \sqrt{4a^2 + 1})^{\frac{p-1}{4}} &= \sqrt{4a^2 + 1} U_{\frac{p-1}{4}}(4a, -1) + \frac{1}{2} V_{\frac{p-1}{4}}(4a, -1) \\ &\equiv \frac{1}{2} V_{\frac{p-1}{4}}(4a, -1) \pmod{p}. \end{aligned}$$

Now the result follows from Theorem 4.1 immediately.

From Theorem 4.1 and (3.3) we deduce the following result.

THEOREM 4.2. *Let $a \in \mathbb{Z}$, $a \neq 0$ and let $p \equiv 1 \pmod{8}$ be a prime such that $p = c^2 + d^2 = x^2 + (4a^2 + 1)y^2$ with $c, d, x, y \in \mathbb{Z}$, $c \equiv 1 \pmod{4}$ and $p \neq 4a^2 + 1$. Suppose $d = 2^r d_0$ with $d_0 \equiv 1 \pmod{4}$. Assume that $(c, x + d) = 1$ or $(d_0, x + c) = 1$. Then*

$$p \mid U_{\frac{p-1}{8}}(4a, -1) \Leftrightarrow 4 \mid xy \text{ and } \frac{p-1}{8} \equiv \begin{cases} \frac{d}{4} + \frac{a}{2}y + \frac{xy}{4} \pmod{2} & \text{if } 2 \mid a, \\ \frac{d}{4} + \frac{y}{4} \pmod{2} & \text{if } 2 \nmid a. \end{cases}$$

REMARK 4.1. We conjecture that the condition $(c, x + d) = 1$ or $(d_0, x + c) = 1$ in Theorems 3.1–3.4, 4.1–4.2 and Corollary 4.1 can be canceled. See also [S4, Conjectures 9.4, 9.10, 9.11, 9.14 and 9.19].

Acknowledgments. The author is supported by the National Natural Sciences Foundation of China (No. 10971078).

References

[BEW] B. C. Berndt, R. J. Evans and K. S. Williams, *Gauss and Jacobi Sums*, Wiley, New York, 1998.

- [IR] K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory*, 2nd ed., Springer, New York, 1990.
- [L] E. Lehmer, *On the quartic character of quadratic units*, J. Reine Angew. Math. 268/269 (1974), 294–301.
- [Lem] F. Lemmermeyer, *Reciprocity Laws: From Euler to Eisenstein*, Springer, Berlin, 2000.
- [S1] Z. H. Sun, *On the theory of cubic residues and nonresidues*, Acta Arith. 84 (1998), 291–335.
- [S2] Z. H. Sun, *Quartic residues and binary quadratic forms*, J. Number Theory 113 (2005), 10–52.
- [S3] Z. H. Sun, *On the quadratic character of quadratic units*, J. Number Theory 128 (2008), 1295–1335.
- [S4] Z. H. Sun, *Quartic, octic residues and Lucas sequences*, J. Number Theory 129 (2009), 499–550.
- [S5] Z. H. Sun, *Congruences for $(A + \sqrt{A^2 + mB^2})^{(p-1)/2}$ and $(b + \sqrt{a^2 + b^2})^{(p-1)/4} \pmod{p}$* , Acta Arith. 149 (2011), 275–296.
- [S6] Z. H. Sun, *Congruences for $q^{\lfloor p/8 \rfloor} \pmod{p}$* , Acta Arith. 159 (2013), 1–25.

Zhi-Hong Sun
School of Mathematical Sciences
Huaiyin Normal University
Huaian, Jiangsu 223001, P.R. China
E-mail: zhihongsun@yahoo.com
<http://www.hytc.edu.cn/xsjl/szh>

Received on 24.9.2012

(7203)