Journal of Number Theory 129 (2009) 499–550

Contents lists available at ScienceDirect

Journal of Number Theory

www.elsevier.com/locate/jnt

Quartic, octic residues and Lucas sequences

Zhi-Hong Sun [1]

Department of Mathematics, Huaiyin Teachers College, Huaian, Jiangsu 223001, PR China

ARTICLE INFO

Article history:
Received 31 December 2006
Available online 11 December 2008
Communicated by David Goss

MSC:
primary 11A15
secondary 11A07, 11B39, 11E25

Keywords:
Lucas sequence
Congruence
Quartic Jacobi symbol

ABSTRACT

Let $p \equiv 1 \pmod 4$ be a prime and $a, b \in \mathbb{Z}$ with $a^2 + b^2 \neq p$. Suppose $p = x^2 + (a^2 + b^2)y^2$ for some integers x and y. In the paper we develop the calculation technique of quartic Jacobi symbols and use it to determine $(\frac{b+\sqrt{a^2+b^2}}{2})^{\frac{p-1}{4}} \pmod p$. As applications we obtain the congruences for $U_{\frac{p-1}{4}}$ modulo p and the criteria for $p \mid U_{\frac{p-1}{8}}$ (if $p \equiv 1 \pmod 8$), where $\{U_n\}$ is the Lucas sequence given by $U_0 = 0$, $U_1 = 1$ and $U_{n+1} = bU_n + k^2 U_{n-1}$ $(n \geqslant 1)$. We also pose many conjectures concerning $U_{\frac{p-1}{4}}$, $m^{\frac{p-1}{8}}$ or $m^{\frac{p-5}{8}} \pmod p$.

1. Introduction

Let $\mathbb{Z}$ and $\mathbb{N}$ be the sets of integers and positive integers respectively, $i = \sqrt{-1}$ and $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$. For $a, b \in \mathbb{Z}$, $a + bi$ is called primary if $b \equiv 0 \pmod 2$ and $a \equiv 1 - b \pmod 4$. When π or $-\pi$ is primary in $\mathbb{Z}[i]$ and $\alpha \in \mathbb{Z}[i]$, one can define the quartic Jacobi symbol $(\frac{\alpha}{\pi})_4$ as in [S4]. For the properties of the quartic Jacobi symbol one may consult [S6, (2.1)–(2.8)].

For any positive odd number m and $a \in \mathbb{Z}$ let $(\frac{a}{m})$ be the (quadratic) Jacobi symbol. (We also assume $(\frac{a}{1}) = 1$.) For our convenience we also define $(\frac{a}{-m}) = (\frac{a}{m})$. Then for any two odd numbers m and n with $m > 0$ or $n > 0$ we have the following general quadratic reciprocity law: $(\frac{m}{n}) = (-1)^{\frac{m-1}{2} \cdot \frac{n-1}{2}} (\frac{n}{m})$.

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

$$U_0(b,c) = 0, \qquad U_1(b,c) = 1,$$
$$U_{n+1}(b,c) = bU_n(b,c) - cU_{n-1}(b,c) \quad (n \geqslant 1) \tag{1.1}$$

E-mail address: szh6174@yahoo.com.

URL: http://www.hytc.edu.cn/xsjl/szh.

[1] The author was supported by Natural Sciences Foundation of Jiangsu Educational Office in China (07KJB110009).

0022-314X/$ – see front matter © 2008 Elsevier Inc. All rights reserved.
doi:10.1016/j.jnt.2008.09.019

and

$$V_0(b,c)=2,\qquad V_1(b,c)=b,$$
$$V_{n+1}(b,c)=bV_n(b,c)-cV_{n-1}(b,c)\quad (n\geqslant 1). \tag{1.2}$$

Let $d=b^2-4c$. It is well known that for $n\in\mathbb{N}$,

$$U_n(b,c)=\begin{cases}\frac{1}{\sqrt{d}}\{(\frac{b+\sqrt{d}}{2})^n-(\frac{b-\sqrt{d}}{2})^n\} & \text{if } d\neq 0,\\ n(\frac{b}{2})^{n-1} & \text{if } d=0\end{cases} \tag{1.3}$$

and

$$V_n(b,c)=\left(\frac{b+\sqrt{d}}{2}\right)^n+\left(\frac{b-\sqrt{d}}{2}\right)^n. \tag{1.4}$$

From [S3, Lemma 6.1(b)] we know that if $p>3$ is a prime such that $p\nmid bcd$, then

$$p\mid U_n(b,c)\iff V_{2n}(b,c)\equiv 2c^n \pmod p. \tag{1.5}$$

Let $F_n=U_n(1,-1)$ and $L_n=V_n(1,-1)$. $\{F_n\}$ and $\{L_n\}$ are called the Fibonacci sequence and Lucas sequence respectively.

Let $b,k\in\mathbb{Z}$ and $(b,k)=1$, where (b,k) is the greatest common divisor of b and k. Let $p\equiv 1 \pmod 4$ be a prime such that $p=x^2+(b^2+4k^2)y^2$ or $x^2+(b^2/4+k^2)y^2$ $(x,y\in\mathbb{Z})$ according as $2\nmid b$ or $2\mid b$. In the paper we develop the calculation technique of quartic Jacobi symbols and use it to determine $(\frac{b+\sqrt{b^2+4k^2}}{2})^{\frac{p-1}{4}} \pmod p$. As applications we obtain the congruences for $U_{\frac{p-1}{4}}(b,-k^2)$ and $V_{\frac{p-1}{4}}(b,-k^2)$ modulo p and the criteria for $p\mid U_{\frac{p-1}{8}}(b,-k^2)$ (if $p\equiv 1 \pmod 8$). These results are concerned with congruences for $(b^2+4k^2)^{[\frac{p}{8}]} \pmod p$, where $[\cdot]$ is the greatest integer function. As examples, we have the following three results.

If $p\equiv 1,9 \pmod{40}$ is a prime and hence $p=C^2+2D^2=x^2+5y^2$ with $C,D,x,y\in\mathbb{Z}$, $C\equiv 1 \pmod 4$, $x=2^\alpha x_0$, $y=2^\beta y_0$ and $x_0\equiv y_0\equiv 1 \pmod 4$, in Section 6 we prove that

$$F_{\frac{p-1}{4}}\equiv\begin{cases}0 \pmod p & \text{if } 2\nmid x,\\ \pm 2(\frac{x}{5})\frac{y}{x} \pmod p & \text{if } 2\mid x \text{ and } x\equiv \pm C,\pm 3C \pmod 5\end{cases} \tag{1.6}$$

and

$$p\mid F_{\frac{p-1}{8}}\iff 2\nmid x \text{ and } x\equiv\begin{cases}C,3C \pmod 5 & \text{if } p\equiv 1,9 \pmod{80},\\ -C,-3C \pmod 5 & \text{if } p\equiv 41,49 \pmod{80}.\end{cases} \tag{1.7}$$

If $p\equiv 3 \pmod 8$ is a prime and $p=x^2+2y^2$ with $x,y\in\mathbb{Z}$, in Section 3 we show that

$$U_{\frac{p+1}{4}}(2,-1)\equiv\big(p-(-1)^{\frac{y^2-1}{8}}\big)/2 \pmod p. \tag{1.8}$$

This confirms a conjecture in [S5].

Let $p\equiv 1,9 \pmod{40}$ be a prime and hence $p=C^2+2D^2=x^2+10y^2$ with $C,D,x,y\in\mathbb{Z}$. Suppose $C\equiv x\equiv 1 \pmod 4$, $y=2^\beta y_0$ and $y_0\equiv 1 \pmod 4$. In Section 8 we show that if $x\equiv\pm C,\pm 3C \pmod 5$, then

$$(3+\sqrt{10})^{\frac{p-1}{4}}\equiv\begin{cases}\pm(-1)^{\frac{C-1}{4}+\frac{y}{4}}(\frac{x}{5}) \pmod p & \text{if } 4\mid y,\\ \mp(-1)^{\frac{C-1}{4}}(\frac{x}{5})\frac{y}{x}\sqrt{10} \pmod p & \text{if } 4\mid y-2.\end{cases} \tag{1.9}$$

For $m \in \mathbb{Z}$ with $m = 2^\alpha m_0 (2 \nmid m_0)$ we say that $2^\alpha \parallel m$ and m_0 is the odd part of m. Let $p \equiv 1 \pmod 4$ be a prime and $p = c^2 + d^2 (c, d \in \mathbb{Z})$ with $c \equiv 1 \pmod 4$. Suppose $a \in \mathbb{Z}$ and $p \nmid a$. In the paper we pose a lot of conjectures on $a^{[p/8]} \pmod p$ (in particular for $a = 3, 5, 7, 13, 17, 37$). For example, if $p \equiv 1 \pmod 8$, b is odd and $p = x^2 + (b^2+4)y^2 \ne b^2 + 4$ $(x, y \in \mathbb{Z})$, then we have good evidence to conjecture that

$$b^2+4 \quad \text{is an octic residue} \pmod p \iff \left(\frac{(2c+bd)/x}{b+2i}\right)_4 = (-1)^{\frac{b-1}{2}+\frac{d}{4}} \delta(y) i, \tag{1.10}$$

where d, x, y are chosen so that the odd parts of d, x, y are of the form $4k+1$ and $\delta(y) = 1$ or -1 according as $8 \mid y$ or not.

If $p \equiv 1, 9 \pmod{20}$ is a prime and $p = c^2 + d^2 = x^2 + 5y^2$ with $c, d, x, y \in \mathbb{Z}$, $c \equiv 1 \pmod 4$ and all the odd parts of d, x, y are of the form $4k+1$, we conjecture that

$$5^{[\frac{p}{8}]} \equiv \begin{cases} \pm(-1)^{\frac{d}{4}} \delta(y) \pmod p & \text{if } p \equiv 1 \pmod 8 \text{ and } x \equiv \pm c \pmod 5, \\ \pm(-1)^{\frac{d}{4}} \delta(y) \frac{d}{c} \pmod p & \text{if } p \equiv 1 \pmod 8 \text{ and } x \equiv \pm d \pmod 5, \\ \pm\delta(x) \frac{dy}{cx} \pmod p & \text{if } p \equiv 5 \pmod 8 \text{ and } x \equiv \pm c \pmod 5, \\ \mp\delta(x) \frac{y}{x} \pmod p & \text{if } p \equiv 5 \pmod 8 \text{ and } x \equiv \pm d \pmod 5. \end{cases} \tag{1.11}$$

From [SS] we know that $p \mid F_{\frac{p-1}{4}}$ if and only if $4 \mid xy$. If $4 \nmid xy$ and (1.11) is true, we can show that

$$F_{\frac{p-1}{4}} \equiv \begin{cases} (-1)^{\frac{d}{4}} \frac{2y}{x} \pmod p & \text{if } 2 \parallel x, \\ \frac{2dy}{cx} \pmod p & \text{if } 2 \parallel y. \end{cases} \tag{1.12}$$

Let $p \equiv 1 \pmod 4$ be a prime, $b \in \mathbb{Z}$, $p \ne b^2+4$, $\frac{b^2}{4}+1$ and $p = x^2 + (b^2+4)y^2$ or $x^2 + (b^2/4+1)y^2$ $(x, y \in \mathbb{Z})$ according as $2 \nmid b$ or $2 \mid b$. In Section 9 we state some conjectures concerning $U_{\frac{p-1}{4}}(b, -1)$ and $V_{\frac{p-1}{4}}(b, -1) \pmod p$ and illustrate that those conjectures are concerned with certain congruences for $(b^2+4)^{[\frac{p}{8}]} \pmod p$. For instance, we conjecture that if $4 \mid y$, then

$$V_{\frac{p-1}{4}}(b, -1) \equiv 2(-1)^{\frac{d}{4}+\frac{y}{4}} \pmod p. \tag{1.13}$$

2. The quartic Jacobi symbol and quartic residuacity

Suppose $a, b \in \mathbb{Z}$, $2 \nmid a$ and $2 \mid b$. Then clearly $(-1)^{\frac{a+b-1}{2}}(a+bi)$ is primary. Thus we may deduce the following properties from [S6, (2.1), (2.3), (2.7)].

Proposition 2.1. *Let $a, b \in \mathbb{Z}$ with $2 \nmid a$ and $2 \mid b$. Then*

$$\left(\frac{i}{a+bi}\right)_4 = i^{\frac{a^2+b^2-1}{4}} = i^{(1-(-1)^{\frac{a+b-1}{2}} a)/2} = (-1)^{\frac{a^2-1}{8}} i^{(1-(-1)^{\frac{b}{2}})/2}$$

and

$$\left(\frac{1+i}{a+bi}\right)_4 = i^{((-1)^{\frac{a-b-1}{2}}(a-b)-1-b^2)/4}$$

$$= \begin{cases} i^{((-1)^{\frac{a-1}{2}}(a-b)-1)/4} & \textit{if } 4 \mid b, \\ i^{\frac{(-1)^{\frac{a-1}{2}}(b-a)-1}{4}-1} & \textit{if } 2 \parallel b. \end{cases}$$

Proposition 2.2. *Let $a, b \in \mathbb{Z}$ with $2 \nmid a$ and $2 \mid b$. Then*

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

Proposition 2.3. *Let $a, b, c, d \in \mathbb{Z}$ with $2 \nmid ac$, $2 \mid b$ and $2 \mid d$. If $a+bi$ and $c+di$ are relatively prime elements of $\mathbb{Z}[i]$, then we have the following general law of quartic reciprocity*:

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

In particular, if $4 \mid b$, we have

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

if $c \equiv 1 \pmod 4$, we have

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

Proof. As $a \equiv c \equiv 1 \pmod 2$ and $b \equiv d \equiv 0 \pmod 2$, we see that $(-1)^{\frac{a+b-1}{2}}(a+bi)$ and $(-1)^{\frac{c+d-1}{2}}(c+di)$ are primary. Hence applying Proposition 2.2 and the general quartic reciprocity law for primary elements (see [IR, Theorem 2, p. 123]) we obtain

$$\begin{aligned}
\left(\frac{a+bi}{c+di}\right)_4 &= \left(\frac{(-1)^{\frac{a+b-1}{2}}(a+bi)}{(-1)^{\frac{c+d-1}{2}}(c+di)}\right)_4 \left(\frac{-1}{c+di}\right)_4^{\frac{a+b-1}{2}} \\
&= (-1)^{\frac{(-1)^{\frac{a+b-1}{2}}a-1}{2}\cdot\frac{(-1)^{\frac{c+d-1}{2}}c-1}{2}}\left(\frac{(-1)^{\frac{c+d-1}{2}}(c+di)}{(-1)^{\frac{a+b-1}{2}}(a+bi)}\right)_4 (-1)^{\frac{d}{2}\cdot\frac{a+b-1}{2}} \\
&= (-1)^{\frac{(-1)^{\frac{b}{2}}-1}{2}\cdot\frac{(-1)^{\frac{d}{2}}-1}{2}}\left(\frac{(-1)^{\frac{c+d-1}{2}}(c+di)}{a+bi}\right)_4 \cdot (-1)^{\frac{d}{2}\cdot\frac{a+b-1}{2}} \\
&= (-1)^{\frac{b}{2}\cdot\frac{d}{2}} \cdot (-1)^{\frac{b}{2}\cdot\frac{c+d-1}{2}}\left(\frac{c+di}{a+bi}\right)_4 \cdot (-1)^{\frac{d}{2}\cdot\frac{a+b-1}{2}}.
\end{aligned}$$

This yields the result. □

Proposition 2.4. *(See [E], [S1, Proposition 1], [S4, Lemma 2.1].) Let $m \in \mathbb{N}$ and $a, b \in \mathbb{Z}$ with $2 \nmid m$ and $(m, a^2+b^2) = 1$. Then*

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

Proposition 2.5. *(See [S7, Lemma 4.3].) Let $a, b \in \mathbb{Z}$ with $2 \nmid a$ and $2 \mid b$. For any integer x with $(x, a^2+b^2) = 1$ we have*

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

Proposition 2.6. *(See [S7, Remark 4.4].) Let $a, b, c, d \in \mathbb{Z}$ with $2 \nmid c$, $2 \mid d$, $(c, d) = 1$ and $(a^2 + b^2, c^2 + d^2) = 1$. Then*

$$\left(\frac{a+bi}{c+di}\right)_4^2 = \left(\frac{ac+bd}{c^2+d^2}\right).$$

For an odd prime q let $F_q = \mathbb{Z}/q\mathbb{Z}$ be the ring of residue classes modulo q and

$$Q(q) = \{\infty\} \cup \left\{x \,\middle|\, x \in F_q,\ x^2 \neq -1\right\}.$$

For $x, y \in Q(q)$, in [S4] the author introduced the operation

$$x * y = \frac{xy-1}{x+y} \quad (x * \infty = \infty * x = x)$$

and proved that $Q(q)$ is a cyclic group of order $q - (\frac{-1}{q})$.

For a given odd prime p let $\mathbb{Z}_p$ denote the set of those rational numbers whose denominator is not divisible by p. Following [S4] we define

$$Q_r(p) = \left\{k \,\middle|\, k \in \mathbb{Z}_p,\ \left(\frac{k+i}{p}\right)_4 = i^r\right\} \quad \text{for } r = 0, 1, 2, 3.$$

Combining [S4, Theorem 2.2] with [S4, Theorem 3.2] (or [S4, Corollary 3.2]) we have the following rational quartic reciprocity law. See also Paul Pollack's talk [P].

Theorem 2.1 *(Rational quartic reciprocity law). Let p and q be distinct odd primes. Suppose $p \equiv 1 \pmod 4$ and $p = a^2 + b^2 (a, b \in \mathbb{Z})$ with $2 \mid b$. Then*

$$\begin{aligned} &(-1)^{\frac{q-1}{2}} q \quad \text{is a quartic residue modulo } p \\ &\iff \frac{a}{b} \quad \text{is a fourth power in } Q(q) \\ &\iff q \mid b \quad \text{or} \quad \frac{a}{b} \equiv \frac{s^4 - 6s^2 + 1}{4s^3 - 4s} \pmod q \quad \text{for some } s \in \mathbb{Z}. \end{aligned}$$

Theorem 2.2. *Let p and q be distinct odd primes. Suppose $p \equiv 1 \pmod 4$ and $p = a^2 + b^2 (a, b \in \mathbb{Z})$ with $a \equiv 1 \pmod 4$ and $q \nmid b$. Let $q^* = (-1)^{\frac{q-1}{2}} q$ and $k \in \mathbb{Z}$ with $(\frac{k+i}{q})_4 = i$. Then*

$$\begin{aligned} &(q^*)^{\frac{p-1}{4}} \equiv \frac{a}{b} \pmod p \\ &\iff \frac{a}{b} \equiv \frac{k(x^4 - 6x^2 + 1) + 4x^3 - 4x}{k(4x^3 - 4x) - (x^4 + 6x^2 + 1)} \pmod q \quad \text{for some } x \in \mathbb{Z}. \end{aligned}$$

Moreover, if $q \not\equiv \pm 1, \pm 9 \pmod{40}$, we may take

$$k = \begin{cases} 1 & \text{if } q \equiv \pm 5 \pmod{16}, \\ -1 & \text{if } q \equiv \pm 3 \pmod{16}, \\ 2 & \text{if } q \equiv \pm 7 \pmod{40}, \\ -2 & \text{if } q \equiv \pm 17 \pmod{40}. \end{cases}$$

Proof. From [S4, Theorem 2.2] we see that

$$(q^*)^{\frac{p-1}{4}} \equiv \left(\frac{b}{a}\right)^3 \pmod p \iff \frac{a}{b} \in Q_3(q).$$

As $(b/a)^3 \equiv a/b \pmod p$ and $-k \in Q_3(q)$, from the above and [S4, Corollaries 3.2 and 3.3] we see that

$$\begin{aligned}
&(q^*)^{\frac{p-1}{4}} \equiv \frac{a}{b} \pmod p \\
&\quad\iff \frac{a}{b} \equiv -k \pmod q \quad \text{or} \quad \frac{a}{b} \equiv \frac{-kk_0-1}{k_0-k} \pmod q \quad \text{for some } k_0 \in Q_0(q) \\
&\quad\iff \frac{a}{b} \equiv -k \pmod q \quad \text{or} \quad \frac{a}{b} \equiv \frac{k(x^4-6x^2+1)/(4x^3-4x)+1}{k-(x^4-6x^2+1)/(4x^3-4x)} \pmod q \quad \text{for some } x \in \mathbb{Z} \\
&\quad\iff \frac{a}{b} \equiv \frac{k(x^4-6x^2+1)+4x^3-4x}{k(4x^3-4x)-(x^4+6x^2+1)} \pmod q \quad \text{for some } x \in \mathbb{Z}.
\end{aligned}$$

If $q \equiv \pm 5 \pmod{16}$, by Proposition 2.1 we have $(\frac{1+i}{q})_4 = i^{((-1)^{\frac{q-1}{2}}q-1)/4} = i$. If $q \equiv \pm 3 \pmod{16}$, by Proposition 2.1 we have $(\frac{-1+i}{q})_4 = (\frac{i}{q})_4(\frac{1+i}{q})_4 = (-1)^{(q^2-1)/8} i^{((-1)^{\frac{q-1}{2}}q-1)/4} = i$. If $q \equiv \pm 7 \pmod{40}$, by Propositions 2.1–2.3 we have

$$\begin{aligned}
\left(\frac{2+i}{q}\right)_4 &= \left(\frac{-i}{q}\right)_4 \left(\frac{-1+2i}{q}\right)_4 = \left(\frac{-1+2i}{q}\right)_4 \\
&= (-1)^{\frac{q-1}{2}} \left(\frac{q}{-1+2i}\right)_4 = -\left(\frac{2}{-1+2i}\right)_4 = i.
\end{aligned}$$

If $q \equiv \pm 17 \pmod{40}$, we have

$$\begin{aligned}
\left(\frac{-2+i}{q}\right)_4 &= \left(\frac{-i}{q}\right)_4 \left(\frac{-1-2i}{q}\right)_4 = \left(\frac{-1-2i}{q}\right)_4 \\
&= (-1)^{\frac{q-1}{2}} \left(\frac{q}{-1-2i}\right)_4 = \left(\frac{2}{-1-2i}\right)_4 = i.
\end{aligned}$$

This completes the proof. □

Theorem 2.3. *(See [S7, Corollary 4.6(i)].) Let $p \equiv 1 \pmod 4$ be a prime and $m \in \mathbb{N}$ with $4 \nmid m$ and $p \nmid m$. Suppose $p = x^2 + my^2$ for some integers x and y. Then*

$$m^{\frac{p-1}{4}} \equiv \begin{cases}
(-1)^{\frac{x-1}{2}}(\frac{x}{m}) \pmod p & \text{if } m \equiv 3 \pmod 4, \\
(\frac{x}{m}) \pmod p & \text{if } m \equiv 1 \pmod 8, \\
(-1)^{x-1}(\frac{x}{m}) \pmod p & \text{if } m \equiv 5 \pmod 8, \\
(-1)^{\frac{x^2-1}{8}+\frac{m-2}{4}\cdot\frac{x-1}{2}}(\frac{x}{m/2}) \pmod p & \text{if } m \equiv 2 \pmod 4.
\end{cases}$$

3. Congruences for $U_{(p-(\frac{-1}{p}))/4}(2,-1)$ and $V_{(p-(\frac{-1}{p}))/4}(2,-1)$ (mod p)

It is clear that

$$1-\sqrt{-1}\cdot\sqrt{-2}=\frac{1}{4}(\sqrt{-1}-1)(\sqrt{-2}-1+\sqrt{-1})^2. \tag{3.1}$$

As $(\sqrt{-1}-1)^2=-2\sqrt{-1}$, for $n\in\mathbb{N}$ we have

$$(1-\sqrt{-1}\cdot\sqrt{-2})^n=\begin{cases}2^{-2n}(-2\sqrt{-1})^{\frac{n}{2}}(\sqrt{-2}-1+\sqrt{-1})^{2n} & \text{if } 2\mid n,\\ 2^{-2n}(\sqrt{-1}-1)(-2\sqrt{-1})^{\frac{n-1}{2}}(\sqrt{-2}-1+\sqrt{-1})^{2n} & \text{if } 2\nmid n.\end{cases} \tag{3.2}$$

Theorem 3.1. *Suppose that $p\equiv 1 \pmod 8$ is a prime and hence $p=c^2+d^2=x^2+2y^2$ for some $c,d,x,y\in\mathbb{Z}$. Suppose $c\equiv x\equiv 1 \pmod 4$. Then*

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

Proof. Taking $n=\frac{p-1}{4}$ in (3.2) we find

$$(1-\sqrt{-1}\cdot\sqrt{-2})^{\frac{p-1}{4}}=2^{\frac{p-1}{8}-\frac{p-1}{2}}(-\sqrt{-1})^{\frac{p-1}{8}}(\sqrt{-2}-1+\sqrt{-1})^{\frac{p-1}{2}}.$$

Set $t=\frac{d}{c}$. As $t^2\equiv -1 \pmod p$ and $(x/y)^2\equiv -2 \pmod p$, by the above we have

$$\left(1-t\frac{x}{y}\right)^{\frac{p-1}{4}}\equiv 2^{\frac{p-1}{8}}(-t)^{\frac{p-1}{8}}\left(\frac{x}{y}-1+t\right)^{\frac{p-1}{2}} \pmod p. \tag{3.3}$$

Suppose $(\frac{\frac{x}{y}-1+i}{p})_4=i^r$. From [S4, Theorem 2.3] we have

$$\left(\frac{\frac{x}{y}-1+t}{\frac{x}{y}-1-t}\right)^{\frac{p-1}{4}}\equiv t^r \pmod p.$$

As

$$\frac{\frac{x}{y}-1+t}{\frac{x}{y}-1-t}=\frac{(\frac{x}{y}-1+t)^2}{(\frac{x}{y}-1)^2-t^2}\equiv\frac{(\frac{x}{y}-1+t)^2}{-2\frac{x}{y}} \pmod p,$$

we see that

$$\left(\frac{x}{y}-1+t\right)^{\frac{p-1}{2}}\equiv\left(-2\frac{x}{y}\right)^{\frac{p-1}{4}}t^r\equiv(-2)^{\frac{p-1}{4}+\frac{p-1}{8}}t^r \pmod p.$$

In view of (3.3) we have

$$\left(1-\frac{tx}{y}\right)^{\frac{p-1}{4}}\equiv(-2)^{\frac{p-1}{8}}t^{\frac{p-1}{8}}\cdot(-2)^{\frac{p-1}{4}+\frac{p-1}{8}}t^r\equiv t^{\frac{p-1}{8}+r} \pmod p.$$

As $p=x^2+2y^2\equiv 1 \pmod 8$ we have $2\mid y$ and $(x-y)^2+y^2=p-2xy$. Suppose $y=2^{\beta}y_0$ with $2\nmid y_0$. Applying Propositions 2.1–2.3 we have

$$\begin{aligned}\left(\frac{\frac{x}{y}-1+i}{p}\right)_4&=\left(\frac{x-y+yi}{p}\right)_4=\left(\frac{p}{x-y+yi}\right)_4=\left(\frac{2xy}{x-y+yi}\right)_4\\&=\left(\frac{2}{x-y+yi}\right)_4^{\beta+1}\left(\frac{x}{x-y+yi}\right)_4\left(\frac{y_0}{x-y+yi}\right)_4\\&=i^{(-1)^{\frac{y}{2}}\frac{y}{2}(\beta+1)}\left(\frac{x-y+yi}{x}\right)_4\cdot(-1)^{\frac{y_0-1}{2}\cdot\frac{y}{2}}\left(\frac{x-y+yi}{y_0}\right)_4\\&=i^{-\frac{y}{2}(\beta+1)}\left(\frac{-y+yi}{x}\right)_4\cdot(-1)^{\frac{y_0-1}{2}\cdot\frac{y}{2}}\left(\frac{x}{y_0}\right)_4\\&=(-1)^{\frac{y_0-1}{2}\cdot\frac{y}{2}}i^{-\frac{y}{2}(\beta+1)}\left(\frac{1-i}{x}\right)_4=(-1)^{\frac{y_0-1}{2}\cdot\frac{y}{2}}i^{-\frac{y}{2}(\beta+1)}\left(\frac{1+i}{x}\right)_4^{-1}\\&=(-1)^{\frac{y_0-1}{2}\cdot\frac{y}{2}}i^{-\frac{y}{2}(\beta+1)}i^{-\frac{x-1}{4}}=\begin{cases}i^{-\frac{x-1}{4}} & \text{if } y\equiv 0,6 \pmod 8,\\ -i^{-\frac{x-1}{4}} & \text{if } y\equiv 2,4 \pmod 8.\end{cases}\end{aligned}$$

Combining the above we obtain

$$\left(1-\frac{tx}{y}\right)^{\frac{p-1}{4}}\equiv\begin{cases}t^{\frac{p-1}{8}-\frac{x-1}{4}} \pmod p & \text{if } y\equiv 0,6 \pmod 8,\\ t^{\frac{p-1}{8}+2-\frac{x-1}{4}}\equiv -t^{\frac{p-1}{8}-\frac{x-1}{4}} \pmod p & \text{if } y\equiv 2,4 \pmod 8.\end{cases}$$

As $p=x^2+2y^2$ we have $\frac{p-1}{8}=\frac{x^2-1}{8}+\frac{y^2}{4}$ and so

$$\begin{aligned}t^{\frac{p-1}{8}-\frac{x-1}{4}}&=t^{\frac{x^2-1}{8}+\frac{y^2}{4}-\frac{x-1}{4}}=t^{\frac{x-1}{4}\cdot\frac{x-1}{2}+\frac{y^2}{4}}\equiv(-1)^{(\frac{x-1}{4})^2}t^{\frac{y^2}{4}}\\&=(-1)^{\frac{x^2-1}{8}}t^{\frac{y^2}{4}}=(-1)^{\frac{p-1}{8}-\frac{y^2}{4}}t^{\frac{y^2}{4}}\equiv(-1)^{\frac{p-1}{8}}(-t)^{4^{\beta-1}} \pmod p.\end{aligned}$$

Thus

$$(-1)^{\frac{p-1}{8}}\left(1-\frac{tx}{y}\right)^{\frac{p-1}{4}}\equiv\begin{cases}1\cdot(-t)^{4^{\beta-1}}\equiv 1 \pmod p & \text{if } y\equiv 0 \pmod 8,\\ -(-t)=t \pmod p & \text{if } y\equiv 2 \pmod 8,\\ -(-t)^4\equiv -1 \pmod p & \text{if } y\equiv 4 \pmod 8,\\ 1\cdot(-t)=-t \pmod p & \text{if } y\equiv 6 \pmod 8.\end{cases}$$

Note that $t=\frac{d}{c}\equiv-\frac{c}{d} \pmod p$. We then obtain the result. □

Corollary 3.1. *Let* $p\equiv 1 \pmod 8$ *be a prime and* $p=x^2+2y^2$ *for some integers* x *and* y*. Then* $1+\sqrt{2}$ *is a quartic residue of* p *if and only if* $p\equiv 2y+1 \pmod{16}$.

Proof. From Theorem 3.1 we see that

$$\begin{aligned}&1+\sqrt{2}\quad\text{is a quartic residue} \pmod p\\&\iff(1+\sqrt{2})^{\frac{p-1}{4}}\equiv 1 \pmod p\iff 4\mid y \text{ and } (-1)^{\frac{p-1}{8}+\frac{y}{4}}=1\\&\iff p\equiv 2y+1 \pmod{16}.\end{aligned}$$

So the result follows. □

Remark 3.1. Using the cyclotomic numbers of order 4, in 1974 E. Lehmer [L2] proved a result equivalent to Corollary 3.1. If $p \equiv 1 \pmod{16}$ is a prime and $p = a^2 + 64b^2 = c^2 + 128d^2$ for some $a, b, c, d \in \mathbb{Z}$, in [L2] Lehmer also showed that $1 + \sqrt{2}$ is an octic residue $\pmod p$ if and only if $b \equiv d \pmod 2$ by using the cyclotomic numbers of order 8.

Theorem 3.2. *Let $p \equiv 3 \pmod 8$ be a prime and hence $p = x^2 + 2y^2$ for some $x, y \in \mathbb{Z}$. Suppose $x \equiv y \pmod 4$. Then*

$$\left(1 - \frac{x}{y}i\right)^{\frac{p+1}{4}} \equiv -(-1)^{\frac{y^2-1}{8}} \frac{1-i}{2} \cdot \frac{x}{y} \pmod p.$$

Proof. Clearly $2 \nmid xy$ and we may assume $x \equiv y \equiv 1 \pmod 4$. Note that $(x/y)^2 \equiv -2 \pmod p$ and $2^{\frac{p-1}{2}} \equiv -1 \pmod p$. Taking $n = (p+1)/4$ in (3.2) we find

$$\begin{aligned}\left(1 - \frac{x}{y}i\right)^{\frac{p+1}{4}} &\equiv 2^{-\frac{p+1}{2}}(i-1)(-2i)^{\frac{p-3}{8}}\left(\frac{x}{y} - 1 + i\right)^{\frac{p+1}{2}} \\ &\equiv 2^{\frac{p-3}{8}-1}(1-i)(-i)^{\frac{p-3}{8}}\left(\frac{x}{y} - 1 + i\right)^{\frac{p+1}{2}} \pmod p.\end{aligned}$$

Suppose $(\frac{\frac{x}{y}-1+i}{p})_4 = i^r$. By [S4, Theorem 2.3] we have

$$\left(\frac{-2\frac{x}{y}}{(\frac{x}{y} - 1 + i)^2}\right)^{\frac{p+1}{4}} \equiv \left(\frac{\frac{x}{y} - 1 - i}{\frac{x}{y} - 1 + i}\right)^{\frac{p+1}{4}} \equiv i^r \pmod p.$$

Hence

$$\left(\frac{x}{y} - 1 + i\right)^{\frac{p+1}{2}} \equiv i^{-r}\left(-2 \cdot \frac{x}{y}\right)^{\frac{p+1}{4}} \equiv (-1)^{\frac{p-3}{8}+1} 2^{\frac{p+1}{4}+\frac{p-3}{8}} i^{-r} \frac{x}{y} \pmod p$$

and so

$$\begin{aligned}\left(1 - \frac{x}{y}i\right)^{\frac{p+1}{4}} &\equiv 2^{\frac{p-3}{8}-1}(1-i)(-i)^{\frac{p-3}{8}} \cdot (-1)^{\frac{p-3}{8}+1} 2^{\frac{p+1}{4}+\frac{p-3}{8}} i^{-r} \frac{x}{y} \\ &\equiv \frac{1-i}{2} \cdot i^{\frac{p-3}{8}-r} \cdot \frac{x}{y} \pmod p.\end{aligned}$$

As $y + (y-x)i$ is primary and $y^2 + (y-x)^2 = p - 2xy$, applying Propositions 2.1–2.3 we have

$$\begin{aligned}\left(\frac{\frac{x}{y} - 1 + i}{p}\right)_4 &= \left(\frac{x - y + yi}{p}\right)_4 = \left(\frac{i}{p}\right)_4 \left(\frac{y + (y-x)i}{p}\right)_4 \\ &= (-1)^{\frac{p^2-1}{8}} \left(\frac{p}{y + (y-x)i}\right)_4 = -\left(\frac{2xy}{y + (y-x)i}\right)_4 \\ &= -\left(\frac{2}{y + (y-x)i}\right)_4 \left(\frac{y + (y-x)i}{x}\right)_4 \left(\frac{y + (y-x)i}{y}\right)_4 \\ &= -i^{\frac{y-x}{2}} \left(\frac{y + yi}{x}\right)_4 \left(\frac{-xi}{y}\right)_4 = -(-1)^{\frac{x-y}{4}} \left(\frac{1+i}{x}\right)_4 \left(\frac{i}{y}\right)_4 \\ &= -(-1)^{\frac{x-y}{4}} i^{\frac{x-1}{4}} \cdot i^{\frac{1-y}{2}} = -(-1)^{\frac{x-1}{4}} i^{\frac{x-1}{4}} = i^{2-\frac{x-1}{4}}.\end{aligned}$$

Hence

$$\left(1-\frac{x}{y}i\right)^{\frac{p+1}{4}} \equiv \frac{1-i}{2}\cdot i^{\frac{p-3}{8}-2+\frac{x-1}{4}}\cdot\frac{x}{y} = -\frac{1-i}{2}\cdot i^{\frac{p-3}{8}+\frac{x-1}{4}}\cdot\frac{x}{y} \pmod{p}.$$

As $p=x^2+2y^2$ we see that $\frac{p-3}{8}=\frac{x^2-1}{8}+\frac{y^2-1}{4}$ and so

$$\begin{aligned} i^{\frac{p-3}{8}+\frac{x-1}{4}} &= i^{\frac{x^2-1}{8}+\frac{y^2-1}{4}+\frac{x-1}{4}} = i^{\frac{x-1}{4}\cdot\frac{x+3}{2}+\frac{y^2-1}{4}} \\ &= (-1)^{\frac{x-1}{4}\cdot\frac{x+3}{4}+\frac{y^2-1}{8}} = (-1)^{\frac{y^2-1}{8}}. \end{aligned}$$

Thus

$$\left(1-\frac{x}{y}i\right)^{\frac{p+1}{4}} \equiv -\frac{1-i}{2}\cdot(-1)^{\frac{y^2-1}{8}}\frac{x}{y} \pmod{p}.$$

This is the result. □

Theorem 3.3. *Suppose that* $p\equiv 1 \pmod 8$ *is a prime and* $p=x^2+2y^2$ *with* $x,y\in\mathbb{Z}$ *and* $x\equiv 1 \pmod 4$. *Then*

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

and

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

Proof. Suppose $p=c^2+d^2$, where $c,d\in\mathbb{Z}$ and $c\equiv 1 \pmod 4$. Observe that $2\mid y$. From Theorem 3.1 we have

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

From (1.3) and (1.4) we have

$$U_n(2,-1)=\frac{1}{2\sqrt{2}}\left\{(1+\sqrt{2})^n-(1-\sqrt{2})^n\right\} \tag{3.4}$$

and

$$V_n(2,-1)=(1+\sqrt{2})^n+(1-\sqrt{2})^n. \tag{3.5}$$

Observe that $(cx/(dy))^2\equiv 2 \pmod p$. We then have

$$\begin{aligned} U_{\frac{p-1}{4}}(2,-1) &\equiv \frac{1}{2cx/(dy)}\left\{\left(1+\frac{cx}{dy}\right)^{\frac{p-1}{4}}-\left(1-\frac{cx}{dy}\right)^{\frac{p-1}{4}}\right\} \\ &\equiv \begin{cases}\frac{1}{2cx/(dy)}\cdot 2(-1)^{\frac{p-1}{8}+\frac{y-2}{4}}\frac{d}{c}\equiv(-1)^{\frac{p-1}{8}+\frac{y+2}{4}}\frac{y}{x} \pmod{p} & \text{if } 4\mid y-2,\\ \frac{1}{2cx/(dy)}((-1)^{\frac{p-1}{8}+\frac{y}{4}}-(-1)^{\frac{p-1}{8}+\frac{y}{4}})=0 \pmod{p} & \text{if } 4\mid y\end{cases} \end{aligned}$$

and

$$\begin{aligned} V_{\frac{p-1}{4}}(2,-1) &\equiv \left(1+\frac{cx}{dy}\right)^{\frac{p-1}{4}} + \left(1-\frac{cx}{dy}\right)^{\frac{p-1}{4}} \\ &\equiv \begin{cases} 0 \pmod p & \text{if } 4 \mid y-2, \\ 2(-1)^{\frac{p-1}{8}+\frac{y}{4}} \pmod p & \text{if } 4 \mid y. \end{cases} \end{aligned}$$

This proves the theorem. □

Theorem 3.4. *Let $p \equiv 1 \pmod 8$ be a prime. Then $p \mid U_{\frac{p-1}{8}}(2,-1)$ if and only if p is represented by x^2+128y^2.*

Proof. Since $p \equiv 1 \pmod 8$ we know that $p = x^2+2y^2$ for some integers x and y. We also have $2 \mid y$ and $(-1)^{\frac{p-1}{8}} = (-1)^{\frac{x^2-1}{8}+\frac{y^2}{4}} = (-1)^{\frac{x^2-1}{8}} \cdot (-1)^{\frac{y}{2}}$. Thus applying (1.5) and Theorem 3.3 we see that

$$\begin{aligned} p \,\big|\, U_{\frac{p-1}{8}}(2,-1) &\iff V_{\frac{p-1}{4}}(2,-1) \equiv 2(-1)^{\frac{p-1}{8}} \pmod p \\ &\iff 4 \mid y \quad\text{and}\quad 2(-1)^{\frac{p-1}{8}+\frac{y}{4}} \equiv 2(-1)^{\frac{p-1}{8}} \pmod p \\ &\iff 8 \mid y. \end{aligned}$$

This yields the result. □

Remark 3.2. Let $p \equiv 1 \pmod 8$ be a prime. From Theorem 3.3 we know that $p \mid U_{\frac{p-1}{4}}(2,-1)$ if and only if $p = x^2+2y^2 (x, y \in \mathbb{Z})$ with $4 \mid y$. This is a known result. See [L2] and [S2]. When $p \equiv 1 \pmod{16}$, Theorem 3.4 was known to E. Lehmer [L2]. In [L2] Lehmer also showed that if $p \equiv 1 \pmod{32}$ is a prime, then $p \mid U_{\frac{p-1}{16}}(2,-1)$ if and only if $p = a^2+64b^2 = c^2+128d^2$ with $a, b, c, d \in \mathbb{Z}$ and $2 \mid b-d$.

Theorem 3.5. *Let $p \equiv 3 \pmod 8$ be a prime and hence $p = x^2+2y^2$ for some $x, y \in \mathbb{Z}$. Suppose $x \equiv y \pmod 4$. Then*

$$U_{\frac{p+1}{4}}(2,-1) \equiv \frac{p-(-1)^{\frac{y^2-1}{8}}}{2} \pmod p$$

and

$$V_{\frac{p+1}{4}}(2,-1) \equiv -(-1)^{\frac{y^2-1}{8}} \frac{x}{y} \pmod p.$$

Proof. From Theorem 3.2 we have

$$\left(1-\frac{x}{y}i\right)^{\frac{p+1}{4}} \equiv -(-1)^{\frac{y^2-1}{8}} \frac{1-i}{2} \cdot \frac{x}{y} \pmod p.$$

Taking conjugates on both sides we obtain

$$\left(1+\frac{x}{y}i\right)^{\frac{p+1}{4}} \equiv -(-1)^{\frac{y^2-1}{8}} \frac{1+i}{2} \cdot \frac{x}{y} \pmod p.$$

Thus, applying (3.4), (3.5) and the fact $(\frac{x}{y}i)^2 \equiv 2 \pmod p$ we see that

$$\begin{aligned} U_{\frac{p+1}{4}}(2,-1) &\equiv \frac{1}{2\cdot\frac{x}{y}i}\left\{\left(1+\frac{x}{y}i\right)^{\frac{p+1}{4}} - \left(1-\frac{x}{y}i\right)^{\frac{p+1}{4}}\right\} \\ &\equiv \frac{1}{2\cdot\frac{x}{y}i}\left\{-(-1)^{\frac{y^2-1}{8}}\frac{1+i}{2}\cdot\frac{x}{y} + (-1)^{\frac{y^2-1}{8}}\frac{1-i}{2}\cdot\frac{x}{y}\right\} \\ &= -\frac{(-1)^{\frac{y^2-1}{8}}}{2} \equiv \frac{p-(-1)^{\frac{y^2-1}{8}}}{2} \pmod p \end{aligned}$$

and

$$\begin{aligned} V_{\frac{p+1}{4}}(2,-1) &\equiv \left(1+\frac{x}{y}i\right)^{\frac{p+1}{4}} + \left(1-\frac{x}{y}i\right)^{\frac{p+1}{4}} \\ &\equiv -(-1)^{\frac{y^2-1}{8}}\frac{1+i}{2}\cdot\frac{x}{y} - (-1)^{\frac{y^2-1}{8}}\frac{1-i}{2}\cdot\frac{x}{y} \\ &= -(-1)^{\frac{y^2-1}{8}}\frac{x}{y} \pmod p. \end{aligned}$$

This proves the theorem. □

Remark 3.3. For a prime $p = x^2 + 2y^2 \equiv 3 \pmod 8$, the congruence $U_{\frac{p+1}{4}}(2,-1) \equiv (p-(-1)^{\frac{y^2-1}{8}})/2 \pmod p$ was conjectured by the author in [S5]. When p is an odd prime, the congruences for $U_{\frac{p\pm1}{2}}(2,-1)$ and $V_{\frac{p\pm1}{2}}(2,-1) \pmod p$ were given by the author in [S2,S5,S7].

4. Congruences for $(-b-a\sqrt{-1})^{\frac{p-(\frac{-1}{p})}{4}}$ (mod p)

Theorem 4.1. *Let $p \equiv 1 \pmod 4$ be a prime and $p = c^2 + d^2$ with $c \equiv 1 \pmod 4$ and $2 \mid d$. Let $a, b \in \mathbb{Z}$, $2 \mid a$, $(a,b) = 1$ and $p \nmid a^2 + b^2$. Suppose $(\frac{ac+bd}{b+ai})_4 = i^k$. Then*

$$\left(-b-a\frac{c}{d}\right)^{\frac{p-1}{4}} \equiv \begin{cases} (-1)^{\frac{b+1}{2}\cdot\frac{d}{2}}(c/d)^k \pmod p & \text{if } 4 \mid a, \\ (-1)^{\frac{b-1}{2}(\frac{d}{2}+1)}(c/d)^{k-1} \pmod p & \text{if } 2 \parallel a. \end{cases}$$

Proof. As $c/d \equiv -i \pmod{c+di}$, we see that

$$\begin{aligned} (-b-ac/d)^{\frac{p-1}{4}} &\equiv (-b+ai)^{\frac{p-1}{4}} \equiv \left(\frac{-b+ai}{c+di}\right)_4 = (-1)^{\frac{a-b-1}{2}\cdot\frac{d}{2}}\left(\frac{c+di}{-b+ai}\right)_4 \\ &= (-1)^{\frac{a-b-1}{2}\cdot\frac{d}{2}}\left(\frac{bc+bdi}{-b+ai}\right)_4\left(\frac{b}{-b+ai}\right)_4^{-1} \\ &= (-1)^{\frac{a-b-1}{2}\cdot\frac{d}{2}}\left(\frac{(ac+bd)i}{-b+ai}\right)_4\cdot(-1)^{\frac{b-1}{2}\cdot\frac{a}{2}}\left(\frac{-b+ai}{b}\right)_4^{-1} \\ &= (-1)^{\frac{a-b-1}{2}\cdot\frac{d}{2}}\left(\frac{ac+bd}{-b+ai}\right)_4(-1)^{\frac{b^2-1}{8}}i^{\frac{1-(-1)^{\frac{a}{2}}}{2}}(-1)^{\frac{b-1}{2}\cdot\frac{a}{2}}\left(\frac{i}{b}\right)_4^{-1} \end{aligned}$$

$$\begin{aligned}
&= (-1)^{\frac{a-b-1}{2}\cdot\frac{d}{2}+\frac{b-1}{2}\cdot\frac{a}{2}} i^{\frac{1-(-1)^{\frac{a}{2}}}{2}} \left(\frac{ac+bd}{b+ai}\right)_4^{-1} \\
&= (-1)^{\frac{a-b-1}{2}\cdot\frac{d}{2}+\frac{b-1}{2}\cdot\frac{a}{2}} i^{\frac{1-(-1)^{\frac{a}{2}}}{2}} i^{-k} \\
&= (-1)^{\frac{a-b-1}{2}\cdot\frac{d}{2}+\frac{b-1}{2}\cdot\frac{a}{2}} (c/d)^{k-(1-(-1)^{\frac{a}{2}})/2} \pmod{c+di}.
\end{aligned}$$

Since $p=(c+di)(c-di)$ we obtain

$$\left(-b-a\frac{c}{d}\right)^{\frac{p-1}{4}} \equiv (-1)^{\frac{a-b-1}{2}\cdot\frac{d}{2}+\frac{b-1}{2}\cdot\frac{a}{2}} (c/d)^{k-(1-(-1)^{\frac{a}{2}})/2} \pmod{p}.$$

This yields the result. □

Corollary 4.1. *Let $p\equiv 1 \pmod 4$ be a prime and $p=c^2+d^2$ with $c\equiv 1 \pmod 4$ and $2\mid d$. Let $a,b\in\mathbb{Z}$, $2\mid b$, $(a,b)=1$ and $p\nmid a^2+b^2$. Suppose $(\frac{ad-bc}{a+bi})_4=i^k$. Then*

$$\left(-b-a\frac{c}{d}\right)^{\frac{p-1}{4}} \equiv \begin{cases} (-1)^{\frac{a+1}{2}\cdot\frac{d}{2}}(c/d)^{\frac{p-1}{4}-k} \pmod p & \text{if } 4\mid b, \\ (-1)^{\frac{a-1}{2}(\frac{d}{2}+1)}(c/d)^{\frac{p-1}{4}-k-1} \pmod p & \text{if } 2\parallel b. \end{cases}$$

Proof. As $(\frac{ad-bc}{a-bi})_4=(\frac{ad-bc}{a+bi})_4^{-1}=i^{-k}$, substituting a,b,k by $-b,a,-k$ in Theorem 4.1 we have

$$\left(-a+b\frac{c}{d}\right)^{\frac{p-1}{4}} \equiv \begin{cases} (-1)^{\frac{a+1}{2}\cdot\frac{d}{2}}(c/d)^{-k} \pmod p & \text{if } 4\mid b, \\ (-1)^{\frac{a-1}{2}(\frac{d}{2}+1)}(c/d)^{-k-1} \pmod p & \text{if } 2\parallel b. \end{cases}$$

Observe that

$$\left(-b-a\frac{c}{d}\right)^{\frac{p-1}{4}} \equiv (c/d)^{\frac{p-1}{4}}\left(-a+b\frac{c}{d}\right)^{\frac{p-1}{4}} \pmod p.$$

By the above we obtain the result. □

Corollary 4.2. *Let $p\equiv 1 \pmod 4$ be a prime and $p\neq 5$. Suppose $p=c^2+d^2$ with $c\equiv 1 \pmod 4$ and $2\mid d$. Then*

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

Proof. Putting $b=1$ and $a=2$ in Theorem 4.1 we see that

$$\left(\frac{2c+d}{1+2i}\right)_4 = i^k \quad\text{implies}\quad \left(-1-2\frac{c}{d}\right)^{\frac{p-1}{4}} \equiv (c/d)^{k-1} \pmod p.$$

As

$$\left(\frac{2c+d}{1+2i}\right)_4 = \begin{cases} \pm i & \text{if } 2c+d\equiv \pm 2 \pmod 5, \\ \mp 1 & \text{if } 2c+d\equiv \pm 4 \pmod 5, \end{cases}$$

we deduce the result. □

Putting $b=-3$ and $a=-2$ in Theorem 4.1 we deduce the following result.

Corollary 4.3. *Let $p\equiv 1\pmod 4$ be a prime and $p\neq 13$. Suppose $p=c^2+d^2$ with $c\equiv 1\pmod 4$ and $2\mid d$. Then*

$$\left(3+2\frac{c}{d}\right)^{\frac{p-1}{4}}\equiv\begin{cases}\pm 1\pmod p & \text{if } 2c+3d\equiv\pm 2,\pm 5,\pm 6\pmod{13},\\ \pm\frac{c}{d}\pmod p & \text{if } 2c+3d\equiv\pm 1,\pm 3,\pm 9\pmod{13}.\end{cases}$$

Putting $b=4$ and $a=1$ in Corollary 4.1 and noting that $(-1)^{\frac{p-1}{4}}=(-1)^{\frac{d}{2}}$ we deduce the following result.

Corollary 4.4. *Let $p\equiv 1\pmod 4$ be a prime and $p\neq 17$. Suppose $p=c^2+d^2$ with $c\equiv 1\pmod 4$ and $2\mid d$. Then*

$$\left(4+\frac{c}{d}\right)^{\frac{p-1}{4}}\equiv\begin{cases}(c/d)^{\frac{p-1}{4}}\pmod p & \text{if } d-4c\equiv\pm 1,\pm 4\pmod{17},\\ -(c/d)^{\frac{p-1}{4}}\pmod p & \text{if } d-4c\equiv\pm 2,\pm 8\pmod{17},\\ (c/d)^{\frac{p-5}{4}}\pmod p & \text{if } d-4c\equiv\pm 6,\pm 7\pmod{17},\\ -(c/d)^{\frac{p-5}{4}}\pmod p & \text{if } d-4c\equiv\pm 3,\pm 5\pmod{17}.\end{cases}$$

Theorem 4.2. *Let $p\equiv 1\pmod 4$ be a prime and $p=c^2+d^2$ with $c\equiv 1\pmod 4$ and $2\mid d$. Suppose $a,b\in\mathbb{Z}$, $2\nmid ab$, $4\mid a+b$, $(a,b)=1$ and $(\frac{\frac{a-b}{2}d-\frac{a+b}{2}c}{\frac{a-b}{2}+\frac{a+b}{2}i})_4=i^k$. Then*

$$(-b-ac/d)^{\frac{p-1}{4}}\equiv(-1)^{\frac{a-1}{2}\cdot\frac{d}{2}+\frac{b-1}{2}\cdot\frac{a+b}{4}}(d/c)^{((-1)^{\frac{d}{2}}(c-d)-1-d^2)/4+(1-(-1)^{\frac{a+b}{4}})/2+k}\pmod p.$$

Proof. As $c/d\equiv -i\pmod{c+di}$ and $b-ai=-(1+i)(\frac{a-b}{2}+\frac{a+b}{2}i)$ we see that

$$\begin{aligned}(b+ac/d)^{\frac{p-1}{4}}&\equiv(b-ai)^{\frac{p-1}{4}}\equiv\left(\frac{b-ai}{c+di}\right)_4=\left(\frac{-1}{c+di}\right)_4\left(\frac{1+i}{c+di}\right)_4\left(\frac{\frac{a-b}{2}+\frac{a+b}{2}i}{c+di}\right)_4\\ &=(-1)^{\frac{d}{2}}i^{((-1)^{\frac{d}{2}}(c-d)-1-d^2)/4}\cdot(-1)^{\frac{a-1}{2}\cdot\frac{d}{2}}\left(\frac{c+di}{\frac{a-b}{2}+\frac{a+b}{2}i}\right)_4\pmod{c+di}.\end{aligned}$$

As

$$\begin{aligned}\left(\frac{c+di}{\frac{a-b}{2}+\frac{a+b}{2}i}\right)_4&=\left(\frac{\frac{a-b}{2}}{\frac{a-b}{2}+\frac{a+b}{2}i}\right)_4^{-1}\left(\frac{\frac{a-b}{2}c+\frac{a-b}{2}di}{\frac{a-b}{2}+\frac{a+b}{2}i}\right)_4\\ &=(-1)^{\frac{(a-b)/2-1}{2}\cdot\frac{(a+b)/2}{2}}\left(\frac{\frac{a-b}{2}+\frac{a+b}{2}i}{\frac{a-b}{2}}\right)_4^{-1}\left(\frac{(\frac{a-b}{2}d-\frac{a+b}{2}c)i}{\frac{a-b}{2}+\frac{a+b}{2}i}\right)_4\\ &=(-1)^{\frac{b-1}{2}\cdot\frac{a+b}{4}}\left(\frac{i}{\frac{a-b}{2}}\right)_4^{-1}\left(\frac{i}{\frac{a-b}{2}+\frac{a+b}{2}i}\right)_4\left(\frac{\frac{a-b}{2}d-\frac{a+b}{2}c}{\frac{a-b}{2}+\frac{a+b}{2}i}\right)_4\\ &=(-1)^{\frac{b-1}{2}\cdot\frac{a+b}{4}}i^{(1-(-1)^{\frac{a+b}{4}})/2}\left(\frac{\frac{a-b}{2}d-\frac{a+b}{2}c}{\frac{a-b}{2}+\frac{a+b}{2}i}\right)_4\\ &=(-1)^{\frac{b-1}{2}\cdot\frac{a+b}{4}}i^{(1-(-1)^{\frac{a+b}{4}})/2+k},\end{aligned}$$

putting the above together with the fact $i \equiv d/c \pmod{c+di}$ we obtain

$$\begin{aligned}\Big(b+a\frac{c}{d}\Big)^{\frac{p-1}{4}} \equiv{}& (-1)^{\frac{d}{2}}\Big(\frac{d}{c}\Big)^{((-1)^{\frac{d}{2}}(c-d)-1-d^2)/4}\cdot(-1)^{\frac{a-1}{2}\cdot\frac{d}{2}}\\ &\times(-1)^{\frac{b-1}{2}\cdot\frac{a+b}{4}}\Big(\frac{d}{c}\Big)^{(1-(-1)^{\frac{a+b}{4}})/2+k} \pmod{c+di}.\end{aligned}$$

This congruence is also true when $c+di$ is replaced by $p=c^2+d^2$. As $(-1)^{\frac{p-1}{4}}=(-1)^{\frac{d}{2}}$, the result follows. □

5. Evaluation of $(\frac{x-ay+byi}{x^2+(a^2+b^2)y^2})_4$

Theorem 5.1. *Let $p \equiv 1 \pmod 4$ be a positive integer and $p = x^2+(a^2+b^2)y^2$ with $a,b,x,y \in \mathbb{Z}$, $(p,axy)=1$, $a=2^r a_0$ $(2\nmid a_0)$, $x=2^\alpha x_0$, $y=2^\beta y_0$ and $x_0 \equiv y_0 \equiv 1 \pmod 4$. Suppose $2\nmid a$ or $2\nmid b$.*

(i) *If $2\mid a$, $2\nmid b$ and $2\mid y$, then*

$$\Big(\frac{x-ay+byi}{p}\Big)_4=\begin{cases}(-1)^{\frac{p-5}{8}+\frac{a_0+1}{2}}i^{br}(\frac{x+byi}{a_0})_4(\frac{x}{b+ai})_4 & \text{if } 2\parallel y,\\ (-1)^{\frac{p-1}{8}+r+1}(\frac{x+byi}{a_0})_4(\frac{x}{b+ai})_4 & \text{if } 8\mid y-4,\\ (-1)^{\frac{p-1}{8}}(\frac{x+byi}{a_0})_4(\frac{x}{b+ai})_4 & \text{if } 8\mid y.\end{cases}$$

(ii) *If $2\nmid a$ and $2\mid b$, then*

$$\Big(\frac{x-ay+byi}{p}\Big)_4=\begin{cases}(\frac{x+byi}{a})_4(\frac{x}{-a+bi})_4 & \text{if } 2\mid y,\\ i^{-\frac{b}{2}}(\frac{x+byi}{a})_4(\frac{x}{-a+bi})_4 & \text{if } 2\nmid y.\end{cases}$$

(iii) *If $2\nmid ab$, then*

$$\Big(\frac{x-ay+byi}{p}\Big)_4=\begin{cases}(-1)^{\frac{a+1}{2}}i^{\frac{x-1}{4}}(\frac{x+byi}{a})_4(\frac{x}{\frac{b-a}{2}+\frac{b+a}{2}i})_4 & \text{if } 4\nmid a-b \text{ and } 2\parallel y,\\ (-1)^{\frac{a+1}{2}}i^{-\frac{x-1}{4}}(\frac{x+byi}{a})_4(\frac{x}{\frac{a+b}{2}+\frac{a-b}{2}i})_4 & \text{if } 4\mid a-b \text{ and } 2\parallel y,\\ (-1)^{\frac{y}{4}}i^{\frac{x-1}{4}}(\frac{x+byi}{a})_4(\frac{x}{\frac{b-a}{2}+\frac{b+a}{2}i})_4 & \text{if } 4\nmid a-b \text{ and } 4\mid y,\\ (-1)^{\frac{y}{4}}i^{-\frac{x-1}{4}}(\frac{x+byi}{a})_4(\frac{x}{\frac{a+b}{2}+\frac{a-b}{2}i})_4 & \text{if } 4\mid a-b \text{ and } 4\mid y.\end{cases}$$

(iv) *If $2\mid a$ and $2\nmid by$, then*

$$\Big(\frac{x-ay+byi}{p}\Big)_4=\begin{cases}(-1)^{\frac{p-b^2}{8}+\frac{a+2}{4}}i^{(-1)^{\frac{b+1}{2}}\frac{a}{2}}(\frac{by-xi}{a_0})_4(\frac{x}{b+ai})_4 & \text{if } 2\parallel a \text{ and } 8\mid p-1,\\ (-1)^{\frac{p-2a-b^2}{8}}(\frac{by-xi}{a_0})_4(\frac{x}{b+ai})_4 & \text{if } 2\parallel a \text{ and } 8\mid p-5,\\ (-1)^{\frac{p-b^2}{8}+(r+1)\frac{a-x}{4}}(\frac{by-xi}{a_0})_4(\frac{x}{b+ai})_4 & \text{if } 4\mid a \text{ and } 8\mid p-1,\\ (-1)^{\frac{p-4a_0-b^2}{8}}i^{(-1)^{\frac{b+1}{2}}r}(\frac{by-xi}{a_0})_4(\frac{x}{b+ai})_4 & \text{if } 4\mid a \text{ and } 8\mid p-5.\end{cases}$$

Proof. We first assume $2 \mid by$. As $(x-ay)^2+(by)^2=p-2axy$ and $(p,2axy)=1$, we see that $2\nmid x-ay$ and so

$$\begin{aligned}\left(\frac{x-ay+byi}{p}\right)_4&=\left(\frac{p}{x-ay+byi}\right)_4=\left(\frac{(x-ay)^2+(by)^2+2axy}{x-ay+byi}\right)_4\\&=\left(\frac{2axy}{x-ay+byi}\right)_4=\left(\frac{2^{1+r+\alpha+\beta}a_0x_0y_0}{x-ay+byi}\right)_4\\&=\left(i^{(-1)^{\frac{x-ay-1}{2}}\frac{by}{2}}\right)^{1+r+\alpha+\beta}(-1)^{\frac{a_0-1}{2}\cdot\frac{by}{2}}\left(\frac{x-ay+byi}{a_0}\right)_4\\&\quad\times\left(\frac{x-ay+byi}{x_0}\right)_4\left(\frac{x-ay+byi}{y_0}\right)_4\\&=(-1)^{\frac{a_0-1}{2}\cdot\frac{by}{2}}i^{(-1)^{\frac{x-ay-1}{2}}\frac{by}{2}(1+r+\alpha+\beta)}\left(\frac{x+byi}{a_0}\right)_4\left(\frac{y(-a+bi)}{x_0}\right)_4\left(\frac{x}{y_0}\right)_4\\&=(-1)^{\frac{a_0-1}{2}\cdot\frac{by}{2}}i^{(-1)^{\frac{x-ay-1}{2}}\frac{by}{2}(1+r+\alpha+\beta)}\left(\frac{x+byi}{a_0}\right)_4\left(\frac{-a+bi}{x_0}\right)_4.\end{aligned}$$

It is easily seen that

$$(-1)^{\frac{a_0-1}{2}\cdot\frac{by}{2}}i^{(-1)^{\frac{x-ay-1}{2}}\frac{by}{2}(1+r+\alpha+\beta)}=\begin{cases}(-1)^{\frac{a-1}{2}\cdot\frac{b}{2}}i^{(-1)^{\frac{x-a-1}{2}}(1+\alpha)\frac{b}{2}} & \text{if } 2\mid b \text{ and } 2\nmid y,\\ (-1)^{\frac{a_0+1}{2}b}i^{(-1)^a br} & \text{if } 2\parallel y,\\ (-1)^{b(r+1)} & \text{if } 4\parallel y,\\ 1 & \text{if } 8\mid y\end{cases}$$

and

$$\left(\frac{-a+bi}{x_0}\right)_4=\begin{cases}\left(\frac{x}{-a+bi}\right)_4 & \text{if } 2\nmid a,\ 2\mid b \text{ and } 2\mid y,\\ \left(\frac{x_0}{-a+bi}\right)_4=\left(\frac{2}{-a+bi}\right)_4^{-\alpha}\left(\frac{x}{-a+bi}\right)_4=i^{(-1)^{\frac{a-1}{2}}\frac{b}{2}\alpha}\left(\frac{x}{-a+bi}\right)_4 & \text{if } 2\nmid a,\ 2\mid b \text{ and } 2\nmid y,\\ \left(\frac{i}{x}\right)_4\left(\frac{b+ai}{x}\right)_4=(-1)^{\frac{x^2-1}{8}}\left(\frac{x}{b+ai}\right)_4 & \text{if } 2\mid a,\ 2\nmid b \text{ and } 2\mid y,\\ \left(\frac{1+i}{x}\right)_4\left(\frac{\frac{b-a}{2}+\frac{b+a}{2}i}{x}\right)_4=i^{\frac{x-1}{4}}\left(\frac{x}{\frac{b-a}{2}+\frac{b+a}{2}i}\right)_4 & \text{if } 2\nmid ab,\ 4\nmid a-b \text{ and } 2\mid y,\\ \left(\frac{i(1+i)}{x}\right)_4\left(\frac{\frac{a+b}{2}+\frac{a-b}{2}i}{x}\right)_4=i^{-\frac{x-1}{4}}\left(\frac{x}{\frac{a+b}{2}+\frac{a-b}{2}i}\right)_4 & \text{if } 2\nmid ab,\ 4\mid a-b \text{ and } 2\mid y.\end{cases}$$

When $a\not\equiv b \pmod 2$ and $2\mid y$, we have $p=x^2+(a^2+b^2)y^2\equiv x^2+y^2 \pmod{16}$ and so $(-1)^{\frac{x^2-1}{8}}=(-1)^{\frac{p-1-y^2}{8}}=(-1)^{[\frac{p}{8}]}$. We also note that $2\nmid ab$ implies $2\mid y$. Now combining the above we deduce (i)–(iii).

Let us consider (iv). Assume $2\nmid by$. Then $y\equiv 1 \pmod 4$. As $p\equiv 1 \pmod 4$ we have $2\mid a$ and $2\mid x$. Since $p=x^2+(a^2+b^2)y^2\equiv x^2+a^2+1 \pmod 8$ we see that $(-1)^{\frac{p-1}{4}}=(-1)^{\frac{a-x}{2}}$. Thus

$$\begin{aligned}
\left(\frac{x-ay+byi}{p}\right)_4 &= \left(\frac{i}{p}\right)_4\left(\frac{by-(x-ay)i}{p}\right)_4 = (-1)^{\frac{p-1}{4}}\left(\frac{p}{by-(x-ay)i}\right)_4 \\
&= (-1)^{\frac{p-1}{4}}\left(\frac{2axy}{by-(x-ay)i}\right)_4 = (-1)^{\frac{p-1}{4}}\left(\frac{2^{r+\alpha+1}a_0x_0y}{by-(x-ay)i}\right)_4 \\
&= (-1)^{\frac{p-1}{4}}\left(\frac{2}{by-(x-ay)i}\right)_4^{r+\alpha+1}\cdot(-1)^{\frac{a_0-1}{2}\cdot\frac{x-ay}{2}}\left(\frac{by-(x-ay)i}{a_0}\right)_4 \\
&\quad\times\left(\frac{by-(x-ay)i}{x_0}\right)_4\left(\frac{by-(x-ay)i}{y}\right)_4 \\
&= (-1)^{\frac{p-1}{4}}i^{(-1)^{\frac{by-1}{2}}(\frac{a}{2}y-\frac{x}{2})(r+\alpha+1)}\cdot(-1)^{\frac{a_0-1}{2}\cdot\frac{x-a}{2}}\left(\frac{by-xi}{a_0}\right)_4 \\
&\quad\times\left(\frac{by+ayi}{x_0}\right)_4\left(\frac{-xi}{y}\right)_4 \\
&= (-1)^{\frac{p-1}{4}+\frac{a_0-1}{2}\cdot\frac{x-a}{2}}i^{(-1)^{\frac{b-1}{2}}\frac{a-x}{2}(r+\alpha+1)}\left(\frac{by-xi}{a_0}\right)_4\left(\frac{b+ai}{x_0}\right)_4\left(\frac{i}{y}\right)_4 \\
&= (-1)^{\frac{p-1}{4}+\frac{y^2-1}{8}+\frac{a_0-1}{2}\cdot\frac{x-a}{2}}i^{(-1)^{\frac{b-1}{2}}\frac{a-x}{2}(r+\alpha+1)}\left(\frac{by-xi}{a_0}\right)_4\left(\frac{x_0}{b+ai}\right)_4 \\
&= (-1)^{\frac{y^2-1}{8}+\frac{a_0+1}{2}\cdot\frac{p-1}{4}}i^{(-1)^{\frac{b-1}{2}}\frac{a-x}{2}(r+\alpha+1)}\left(\frac{by-xi}{a_0}\right)_4\left(\frac{2^{-\alpha}x}{b+ai}\right)_4 \\
&= (-1)^{\frac{y^2-1}{8}+\frac{a_0+1}{2}\cdot\frac{p-1}{4}}i^{(-1)^{\frac{b-1}{2}}(\frac{a-x}{2}(r+\alpha+1)-\frac{a}{2}\alpha)}\left(\frac{by-xi}{a_0}\right)_4\left(\frac{x}{b+ai}\right)_4.
\end{aligned}$$

Observe that

$$\begin{aligned}
(-1)^{\frac{y^2-1}{8}} = (-1)^{\frac{(a^2+b^2)y^2-(a^2+b^2)}{8}} &= (-1)^{\frac{p-x^2-a^2-b^2}{8}} \\
&= \begin{cases} (-1)^{\frac{p-b^2}{8}+\frac{a}{2}} & \text{if } p\equiv 1 \pmod 8, \\ (-1)^{\frac{p-4-b^2}{8}} & \text{if } p\equiv 5 \pmod 8. \end{cases}
\end{aligned}$$

By the above we obtain

$$\left(\frac{x-ay+byi}{p}\right)_4 = \begin{cases} (-1)^{\frac{p-b^2}{8}+\frac{a}{2}+\frac{a-x}{4}(r+\alpha+1)}i^{(-1)^{\frac{b+1}{2}}\frac{a}{2}\alpha}\left(\frac{by-xi}{a_0}\right)_4\left(\frac{x}{b+ai}\right)_4 & \text{if } 8\mid p-1, \\ (-1)^{\frac{p+4a_0-b^2}{8}}i^{(-1)^{\frac{b-1}{2}}(\frac{a-x}{2}(r+\alpha+1)-\frac{a}{2}\alpha)}\left(\frac{by-xi}{a_0}\right)_4\left(\frac{x}{b+ai}\right)_4 & \text{if } 8\mid p-5. \end{cases}$$

This yields (iv) and hence the theorem is proved. □

6. Congruences for $U_{\frac{p-1}{4}}(b,-k^2)$ and $V_{\frac{p-1}{4}}(b,-k^2)$ (mod p) when $2\nmid b$

For two numbers a and b it is easily seen that

$$(-b-ai)\cdot\frac{b-i\sqrt{-a^2-b^2}}{2} = \left(\frac{\sqrt{-a^2-b^2}-a+bi}{2}\right)^2. \tag{6.1}$$

This is the starting point for our purpose in the section.

Lemma 6.1. *Let $p \equiv 1 \pmod 4$ be a prime and $t^2 \equiv -1 \pmod p$ $(t \in \mathbb{Z})$. Suppose $a, b, s \in \mathbb{Z}$, $s^2 \equiv -a^2 - b^2 \pmod p$ and $p \nmid a^2 + b^2$. If $(\frac{s-a+bi}{p})_4 = i^r$, then*

$$\begin{aligned}(s-a+bt)^{\frac{p-1}{2}} &\equiv (-2as)^{\frac{p-1}{4}} t^r \\ &\equiv \begin{cases} (2a)^{\frac{p-1}{4}}(-a^2-b^2)^{\frac{p-1}{8}} t^r \pmod p & \text{if } 8 \mid p-1, \\ -(2a)^{\frac{p-1}{4}}(-a^2-b^2)^{\frac{p-5}{8}} st^r \pmod p & \text{if } 8 \mid p-5. \end{cases}\end{aligned}$$

Proof. If $p \mid b$, then $s \equiv \pm at \pmod p$. Observing that $2^{\frac{p-1}{2}} \equiv (-1)^{\frac{p-1}{4}} \pmod p$ and $t^2 \equiv -1 \pmod p$ we deduce the result. Now assume $p \nmid b$. From [S4, Theorem 2.3] we know that for $k \in \mathbb{Z}_p$ with $k^2 + 1 \not\equiv 0 \pmod p$,

$$\begin{aligned} k \in Q_r(p) &\iff \left(\frac{k+t}{k-t}\right)^{\frac{p-1}{4}} \equiv t^r \pmod p \\ &\iff (k+t)^{\frac{p-1}{2}} \equiv \big(k^2+1\big)^{\frac{p-1}{4}} t^r \pmod p. \end{aligned} \tag{6.2}$$

Now suppose $(\frac{s-a+bi}{p})_4 = i^r$. That is, $\frac{s-a}{b} \in Q_r(p)$. Note that

$$\frac{(s-a)^2}{b^2} + 1 = \frac{s^2+a^2+b^2-2as}{b^2} \equiv -\frac{2as}{b^2} \pmod p.$$

Taking $k = \frac{s-a}{b}$ in (6.2) we then have

$$\left(\frac{s-a}{b} + t\right)^{\frac{p-1}{2}} \equiv \left(-\frac{2as}{b^2}\right)^{\frac{p-1}{4}} t^r \pmod p.$$

That is,

$$(s-a+bt)^{\frac{p-1}{2}} \equiv (-2as)^{\frac{p-1}{4}} t^r \pmod p.$$

As $s^2 \equiv -a^2 - b^2 \pmod p$ we deduce the remaining result. □

Theorem 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 $a, b \in \mathbb{Z}$, $2 \mid a$, $(a, b) = 1$ and $a = 2^r a_0 (2 \nmid a_0)$. Assume $p = x^2 + (a^2 + b^2)y^2$ with $x, y \in \mathbb{Z}$, $x = 2^\alpha x_0$, $y = 2^\beta y_0$ and $x_0 \equiv y_0 \equiv 1 \pmod 4$. Suppose $(\frac{x-byi}{a_0})_4 (\frac{(ac+bd)/x}{b+ai})_4 = i^n$.*

(i) *If $2 \mid y$, then*

$$\left(\frac{b-cx/(dy)}{2}\right)^{\frac{p-1}{4}} \equiv \begin{cases} (-1)^{\frac{a/2+b}{2}} (d/c)^n \frac{x}{y} (\frac{a}{2})^{\frac{p-1}{4}} (a^2+b^2)^{\frac{p-5}{8}} \pmod p & \text{if } 2 \parallel a \text{ and } 2 \parallel y, \\ (-1)^{\frac{b-1}{2}} (d/c)^{n-1} (\frac{a}{2})^{\frac{p-1}{4}} (a^2+b^2)^{\frac{p-1}{8}} \pmod p & \text{if } 2 \parallel a \text{ and } 4 \mid y, \\ (-1)^{\frac{a_0+b}{2}} (d/c)^{n-br} \frac{x}{y} (\frac{a}{2})^{\frac{p-1}{4}} (a^2+b^2)^{\frac{p-5}{8}} \pmod p & \text{if } 4 \mid a \text{ and } 2 \parallel y, \\ (-1)^{(r+1)\frac{y}{4}} (d/c)^n (\frac{a}{2})^{\frac{p-1}{4}} (a^2+b^2)^{\frac{p-1}{8}} \pmod p & \text{if } 4 \mid a \text{ and } 4 \mid y. \end{cases}$$

(ii) *If* $2 \nmid y$, *then*

$$\Big(\frac{b-cx/(dy)}{2}\Big)^{\frac{p-1}{4}} \equiv \begin{cases} -(-1)^{\frac{a^2/4-b^2}{8}}(d/c)^n(\frac{a}{2})^{\frac{p-1}{4}}(a^2+b^2)^{\frac{p-1}{8}} \pmod p \\ \quad \textit{if } 2 \parallel a \textit{ and } 2 \parallel x, \\ (-1)^{\frac{a+2}{4}+\frac{a^2/4-b^2}{8}}(d/c)^{n-1}\frac{x}{y}(\frac{a}{2})^{\frac{p-1}{4}}(a^2+b^2)^{\frac{p-5}{8}} \pmod p \\ \quad \textit{if } 2 \parallel a \textit{ and } 4 \mid x, \\ (-1)^{\frac{a_0^2-b^2}{8}+(r+1)\frac{a-x}{4}}(d/c)^n(\frac{a}{2})^{\frac{p-1}{4}}(a^2+b^2)^{\frac{p-1}{8}} \pmod p \\ \quad \textit{if } 4 \mid a \textit{ and } 4 \mid x, \\ (-1)^{\frac{(a_0+2)^2-(b+2)^2}{8}}(d/c)^{n+(-1)^{\frac{b-1}{2}}r}\frac{x}{y}(\frac{a}{2})^{\frac{p-1}{4}}(a^2+b^2)^{\frac{p-5}{8}} \pmod p \\ \quad \textit{if } 4 \mid a \textit{ and } 2 \parallel x. \end{cases}$$

Proof. Suppose $(\frac{ac+bd}{b+ai})_4 = i^k$ and $(\frac{x+byi}{a_0})_4(\frac{x}{b+ai})_4 = i^m$. Then $\big(\frac{x-byi}{a_0})_4\ (\frac{1/x}{b+ai})_4 = i^{-m}$ and so $i^{k-m} = i^n$. As $(c/d)^2 \equiv -1 \pmod p$ and $(x/y)^2 \equiv -a^2-b^2 \pmod p$, by (6.1) we have

$$\Big(-b-a\frac{c}{d}\Big)\frac{b-\frac{c}{d}\cdot\frac{x}{y}}{2} \equiv \Big(\frac{\frac{x}{y}-a+b\frac{c}{d}}{2}\Big)^2 \pmod p.$$

Thus

$$\Big(\frac{b-cx/(dy)}{2}\Big)^{\frac{p-1}{4}} \equiv \Big(\frac{\frac{x}{y}-a+b\frac{c}{d}}{2}\Big)^{\frac{p-1}{2}}\Big(-b-a\frac{c}{d}\Big)^{-\frac{p-1}{4}} \pmod p. \tag{6.3}$$

By Theorem 4.1 we have

$$\Big(-b-a\frac{c}{d}\Big)^{-\frac{p-1}{4}} \equiv \begin{cases} (-1)^{\frac{b+1}{2}\cdot\frac{d}{2}}(c/d)^{-k} \pmod p & \text{if } 4 \mid a, \\ (-1)^{\frac{b-1}{2}(\frac{d}{2}+1)}(c/d)^{1-k} \pmod p & \text{if } 2 \parallel a. \end{cases} \tag{6.4}$$

If $2 \mid y$, by Theorem 5.1(i) we have

$$\Big(\frac{\frac{x}{y}-a+bi}{p}\Big)_4 = \Big(\frac{x-ay+byi}{p}\Big)_4 = \begin{cases} (-1)^{\frac{p-5}{8}+\frac{a_0+1}{2}} i^{br+m} & \text{if } 2 \parallel y, \\ (-1)^{\frac{p-1}{8}+(r+1)\frac{y}{4}} i^m & \text{if } 4 \mid y. \end{cases}$$

Hence appealing to Lemma 6.1 we obtain

$$\Big(\frac{x}{y}-a+b\frac{c}{d}\Big)^{\frac{p-1}{2}} \equiv \begin{cases} (-1)^{\frac{a_0-1}{2}}(c/d)^{br+m}(2a)^{\frac{p-1}{4}}(a^2+b^2)^{\frac{p-5}{8}}\frac{x}{y} \pmod p & \text{if } 2 \parallel y, \\ (-1)^{(r+1)\frac{y}{4}}(c/d)^m(2a)^{\frac{p-1}{4}}(a^2+b^2)^{\frac{p-1}{8}} \pmod p & \text{if } 4 \mid y. \end{cases}$$

Combining this with (6.3), (6.4) and the fact $(c/d)^{m-k} = (d/c)^{k-m} \equiv (d/c)^n \pmod p$ yields (i).

Now assume $2 \nmid y$. As $(\frac{by-xi}{a_0})_4(\frac{x}{b+ai})_4 = (\frac{-i}{a_0})_4(\frac{x+byi}{a_0})_4(\frac{x}{b+ai})_4 = (-1)^{\frac{a_0^2-1}{8}} i^m$, by Theorem 5.1(iv) we have

$$\left(\frac{\frac{x}{y}-a+bi}{p}\right)_4 = \left(\frac{x-ay+byi}{p}\right)_4 = \begin{cases} (-1)^{\frac{p-b^2}{8}+\frac{a+2}{4}+\frac{a_0^2-1}{8}} i^{(-1)^{\frac{b+1}{2}}\frac{a}{2}+m} & \text{if } 2 \parallel a \text{ and } 8 \mid p-1, \\ (-1)^{\frac{p-2a-b^2}{8}+\frac{a_0^2-1}{8}} i^m & \text{if } 2 \parallel a \text{ and } 8 \mid p-5, \\ (-1)^{\frac{p-b^2}{8}+(r+1)\frac{a-x}{4}+\frac{a_0^2-1}{8}} i^m & \text{if } 4 \mid a \text{ and } 8 \mid p-1, \\ (-1)^{\frac{p-4a_0-b^2}{8}+\frac{a_0^2-1}{8}} i^{(-1)^{\frac{b+1}{2}}r+m} & \text{if } 4 \mid a \text{ and } 8 \mid p-5. \end{cases}$$

Applying Lemma 6.1 we see that

$$\left(\frac{x}{y}-a+b\frac{c}{d}\right)^{\frac{p-1}{2}} \equiv \begin{cases} (-1)^{\frac{p-b^2}{8}+\frac{a+2}{4}+\frac{a_0^2-1}{8}}(2a)^{\frac{p-1}{4}}(-a^2-b^2)^{\frac{p-1}{8}}(c/d)^{(-1)^{\frac{b+1}{2}}\frac{a}{2}+m} \\ \quad \text{if } 2 \parallel a \text{ and } 8 \mid p-1, \\ -(-1)^{\frac{p-2a-b^2}{8}+\frac{a_0^2-1}{8}}(2a)^{\frac{p-1}{4}}(-a^2-b^2)^{\frac{p-5}{8}}\frac{x}{y}(c/d)^m \\ \quad \text{if } 2 \parallel a \text{ and } 8 \mid p-5, \\ (-1)^{\frac{p-b^2}{8}+(r+1)\frac{a-x}{4}+\frac{a_0^2-1}{8}}(2a)^{\frac{p-1}{4}}(-a^2-b^2)^{\frac{p-1}{8}}(c/d)^m \\ \quad \text{if } 4 \mid a \text{ and } 8 \mid p-1, \\ -(-1)^{\frac{p-4a_0-b^2}{8}+\frac{a_0^2-1}{8}}(2a)^{\frac{p-1}{4}}(-a^2-b^2)^{\frac{p-5}{8}}\frac{x}{y}(c/d)^{(-1)^{\frac{b+1}{2}}r+m} \\ \quad \text{if } 4 \mid a \text{ and } 8 \mid p-5. \end{cases}$$

As $(-1)^{\frac{p-1}{4}} = (-1)^{\frac{a}{2}+\frac{x}{2}}$ and $(c/d)^{m-k} = (d/c)^{k-m} \equiv (d/c)^n \pmod p$, combining the above with (6.3) and (6.4) yields (ii). So the theorem is proved. □

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 $x, y \in \mathbb{Z}$, $x = 2^\alpha x_0$, $y = 2^\beta y_0$ and $x_0 \equiv y_0 \equiv 1 \pmod 4$. Then*

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

Corollary 6.2. *Let $p \equiv 1, 9 \pmod{20}$ be a prime and hence $p = c^2 + d^2 = x^2 + 5y^2$ for some $c, d, x, y \in \mathbb{Z}$. Suppose $c \equiv 1 \pmod 4$, $x = 2^\alpha x_0$, $y = 2^\beta y_0$ and $x_0 \equiv y_0 \equiv 1 \pmod 4$. Then*

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

Proof. Since $(\frac{5}{p}) = 1$, it is well known that $5 \mid cd$ (see [S4, Theorem 2.2 and Example 2.1]). Clearly $5 \mid c$ if and only if $x \equiv \pm d \pmod 5$, and $5 \mid d$ if and only if $x \equiv \pm c \pmod 5$. Thus

$$\left(\frac{(2c+d)/x}{1+2i}\right)_4 = \begin{cases} (\frac{\pm 1}{1+2i})_4 = \pm 1 & \text{if } x \equiv \pm d \pmod 5, \\ (\frac{\pm 2}{1+2i})_4 = \pm i & \text{if } x \equiv \pm c \pmod 5. \end{cases} \tag{6.5}$$

Now taking $b = 1$ in Corollary 6.1 and then applying (6.5) we obtain the result. □

Observe that

$$\left(\frac{m}{3+2i}\right)_4 = \begin{cases} \pm 1 & \text{if } m \equiv \pm 1, \pm 3, \pm 9 \pmod{13}, \\ \pm i & \text{if } m \equiv \mp 2, \mp 5, \mp 6 \pmod{13}. \end{cases} \tag{6.6}$$

Putting $b = 3$ in Theorem 6.1 we obtain:

Corollary 6.3. *Let $p \equiv 1, 9, 17, 25, 29, 49 \pmod{52}$ be a prime and hence $p = c^2 + d^2 = x^2 + 13y^2$ for some $c, d, x, y \in \mathbb{Z}$. Suppose $c \equiv 1 \pmod 4$, $x = 2^\alpha x_0$, $y = 2^\beta y_0$ and $x_0 \equiv y_0 \equiv 1 \pmod 4$. Then*

$$\left(\frac{3 - \frac{cx}{dy}}{2}\right)^{\frac{p-1}{4}} \equiv \begin{cases} \pm 13^{\frac{p-1}{8}} \pmod p & \text{if } 4 \mid y \text{ and } \frac{2c+3d}{x} \equiv \pm 2, \pm 5, \pm 6 \pmod{13}, \\ & \text{or if } 2 \parallel x \text{ and } \frac{2c+3d}{x} \equiv \pm 1, \pm 3, \pm 9 \pmod{13}, \\ \pm 13^{\frac{p-1}{8}} \frac{d}{c} \pmod p & \text{if } 4 \mid y \text{ and } \frac{2c+3d}{x} \equiv \pm 1, \pm 3, \pm 9 \pmod{13}, \\ & \text{or if } 2 \parallel x \text{ and } \frac{2c+3d}{x} \equiv \mp 2, \mp 5, \mp 6 \pmod{13}, \\ \pm 13^{\frac{p-5}{8}} \frac{x}{y} \pmod p & \text{if } 2 \parallel y \text{ and } \frac{2c+3d}{x} \equiv \pm 1, \pm 3, \pm 9 \pmod{13}, \\ & \text{or if } 4 \mid x \text{ and } \frac{2c+3d}{x} \equiv \mp 2, \mp 5, \mp 6 \pmod{13}, \\ \pm 13^{\frac{p-5}{8}} \frac{dx}{cy} \pmod p & \text{if } 2 \parallel y \text{ and } \frac{2c+3d}{x} \equiv \mp 2, \mp 5, \mp 6 \pmod{13}, \\ & \text{or if } 4 \mid x \text{ and } \frac{2c+3d}{x} \equiv \mp 1, \mp 3, \mp 9 \pmod{13}. \end{cases}$$

Theorem 6.2. *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 $b, k \in \mathbb{Z}$, $2 \nmid b$, $(b, k) = 1$ and $2k = 2^r k_0 (2 \nmid k_0)$. Assume $p = x^2 + (b^2 + 4k^2)y^2$ with $x, y \in \mathbb{Z}$, $x = 2^\alpha x_0$, $y = 2^\beta y_0$ and $x_0 \equiv y_0 \equiv 1 \pmod 4$. Suppose $(\frac{x - byi}{k_0})_4 (\frac{(2kc+bd)/x}{b+2ki})_4 = i^n$.*

(i) *If* $2\nmid k$, *then*

$$U_{\frac{p-1}{4}}(b,-k^2)\equiv\begin{cases}((\frac{k}{p})+1)(-1)^{\frac{k-b}{2}}(d/c)^{n+1}k^{\frac{p-1}{4}}(b^2+4k^2)^{\frac{p-5}{8}}\pmod p & \text{if } 2\parallel y,\\ ((\frac{k}{p})-1)(-1)^{\frac{b-1}{2}}(d/c)^{n}\frac{y}{x}k^{\frac{p-1}{4}}(b^2+4k^2)^{\frac{p-1}{8}}\pmod p & \text{if } 4\mid y,\\ ((\frac{k}{p})+1)(-1)^{\frac{k^2-b^2}{8}}(d/c)^{n+1}\frac{y}{x}k^{\frac{p-1}{4}}(b^2+4k^2)^{\frac{p-1}{8}}\pmod p & \text{if } 2\parallel x,\\ ((\frac{k}{p})-1)(-1)^{\frac{(k+2)^2-b^2}{8}}(d/c)^{n}k^{\frac{p-1}{4}}(b^2+4k^2)^{\frac{p-5}{8}}\pmod p & \text{if } 4\mid x\end{cases}$$

and

$$V_{\frac{p-1}{4}}(b,-k^2)\equiv\begin{cases}((\frac{k}{p})-1)(-1)^{\frac{k-b}{2}}(d/c)^{n}\frac{x}{y}k^{\frac{p-1}{4}}(b^2+4k^2)^{\frac{p-5}{8}}\pmod p & \text{if } 2\parallel y,\\ ((\frac{k}{p})+1)(-1)^{\frac{b-1}{2}}(d/c)^{n-1}k^{\frac{p-1}{4}}(b^2+4k^2)^{\frac{p-1}{8}}\pmod p & \text{if } 4\mid y,\\ ((\frac{k}{p})-1)(-1)^{\frac{k^2-b^2}{8}}(d/c)^{n}k^{\frac{p-1}{4}}(b^2+4k^2)^{\frac{p-1}{8}}\pmod p & \text{if } 2\parallel x,\\ ((\frac{k}{p})+1)(-1)^{\frac{(k+2)^2-b^2}{8}}(d/c)^{n-1}\frac{x}{y}k^{\frac{p-1}{4}}(b^2+4k^2)^{\frac{p-5}{8}}\pmod p & \text{if } 4\mid x.\end{cases}$$

(ii) *If* $2\mid k$, *then*

$$U_{\frac{p-1}{4}}\big(b,-k^2\big)$$
$$\equiv\begin{cases}(1+(\frac{k}{p}))(-1)^{\frac{k_0-b}{2}}(d/c)^{n+1-br}k^{\frac{p-1}{4}}(b^2+4k^2)^{\frac{p-5}{8}}\pmod p & \text{if } 2\parallel y,\\ ((\frac{k}{p})-1)(-1)^{(r+1)\frac{y}{4}}(d/c)^{n+1}\frac{y}{x}k^{\frac{p-1}{4}}(b^2+4k^2)^{\frac{p-1}{8}}\pmod p & \text{if } 4\mid y,\\ -(1+(\frac{k}{p}))(-1)^{\frac{(k_0+2)^2-(b+2)^2}{8}}(d/c)^{n+1+(-1)^{\frac{b-1}{2}}r}k^{\frac{p-1}{4}}(b^2+4k^2)^{\frac{p-5}{8}}\pmod p & \text{if } 2\parallel x,\\ ((\frac{k}{p})-1)(-1)^{(r+1)\frac{2k-x}{4}+\frac{k_0^2-b^2}{8}}(d/c)^{n+1}\frac{y}{x}k^{\frac{p-1}{4}}(b^2+4k^2)^{\frac{p-1}{8}}\pmod p & \text{if } 4\mid x\end{cases}$$

and

$$V_{\frac{p-1}{4}}\big(b,-k^2\big)$$
$$\equiv\begin{cases}(1-(\frac{k}{p}))(-1)^{\frac{k_0+b}{2}}(d/c)^{n-br}\frac{x}{y}k^{\frac{p-1}{4}}(b^2+4k^2)^{\frac{p-5}{8}}\pmod p & \text{if } 2\parallel y,\\ (1+(\frac{k}{p}))(-1)^{(r+1)\frac{y}{4}}(d/c)^{n}k^{\frac{p-1}{4}}(b^2+4k^2)^{\frac{p-1}{8}}\pmod p & \text{if } 4\mid y,\\ (1-(\frac{k}{p}))(-1)^{\frac{(k_0+2)^2-(b+2)^2}{8}}(d/c)^{n+(-1)^{\frac{b-1}{2}}r}\frac{x}{y}k^{\frac{p-1}{4}}(b^2+4k^2)^{\frac{p-5}{8}}\pmod p & \text{if } 2\parallel x,\\ (1+(\frac{k}{p}))(-1)^{(r+1)\frac{2k-x}{4}+\frac{k_0^2-b^2}{8}}(d/c)^{n}k^{\frac{p-1}{4}}(b^2+4k^2)^{\frac{p-1}{8}}\pmod p & \text{if } 4\mid x.\end{cases}$$

Proof. Set $a=2k$. Using Propositions 2.4 and 2.5 we see that

$$\begin{aligned}&\left(\frac{x-byi}{k_0}\right)_4\left(\frac{(ac+bd)/x}{b+ai}\right)_4\cdot\left(\frac{x-byi}{k_0}\right)_4\left(\frac{(ac-bd)/x}{b+ai}\right)_4\\ &\quad=\left(\frac{x^2+b^2y^2}{k_0}\right)\left(\frac{x^2}{b+ai}\right)_4^{-1}\left(\frac{a^2c^2-b^2d^2}{b+ai}\right)_4\\ &\quad=\left(\frac{p-4k^2y^2}{k_0}\right)\left(\frac{x^2}{b+ai}\right)_4\left(\frac{-b^2(c^2+d^2)}{b+ai}\right)_4\end{aligned}$$

$$\begin{aligned}&=\left(\frac{p}{k_0}\right)\left(\frac{x^2}{b+ai}\right)_4\cdot(-1)^{\frac{a}{2}}\left(\frac{b}{a^2+b^2}\right)\left(\frac{x^2+(a^2+b^2)y^2}{b+ai}\right)_4\\&=(-1)^k\left(\frac{k_0}{p}\right)\left(\frac{a^2+b^2}{b}\right)\left(\frac{x^2}{b+ai}\right)_4\left(\frac{x^2}{b+ai}\right)_4\\&=(-1)^k\left(\frac{k_0}{p}\right).\end{aligned}$$

Thus,

$$\begin{aligned}\left(\frac{x-byi}{k_0}\right)_4\left(\frac{(ac-bd)/x}{b+ai}\right)_4&=(-1)^k\left(\frac{k_0}{p}\right)\left(\frac{x-byi}{k_0}\right)_4^{-1}\left(\frac{(ac+bd)/x}{b+ai}\right)_4^{-1}\\&=(-1)^k\left(\frac{k_0}{p}\right)i^{-n}=i^{1-(-1)^k(\frac{k_0}{p})-n}.\end{aligned}$$

We note that

$$\left(\frac{k_0}{p}\right)=\left(\frac{2k/2^r}{p}\right)=\left(\frac{2}{p}\right)^{r-1}\left(\frac{k}{p}\right)=(-1)^{\frac{p-1}{4}(r-1)}\left(\frac{k}{p}\right).$$

As $(\frac{cx}{dy})^2\equiv a^2+b^2\pmod p$, by (1.3) and (1.4) we have

$$U_{\frac{p-1}{4}}\left(b,-k^2\right)\equiv\frac{1}{cx/(dy)}\left\{\left(\frac{b+\frac{cx}{dy}}{2}\right)^{\frac{p-1}{4}}-\left(\frac{b-\frac{cx}{dy}}{2}\right)^{\frac{p-1}{4}}\right\}\pmod p \tag{6.7}$$

and

$$V_{\frac{p-1}{4}}\left(b,-k^2\right)\equiv\left(\frac{b+\frac{cx}{dy}}{2}\right)^{\frac{p-1}{4}}+\left(\frac{b-\frac{cx}{dy}}{2}\right)^{\frac{p-1}{4}}\pmod p. \tag{6.8}$$

If $2\nmid k$ and $2\parallel y$, then $2\parallel a$ and $k_0=k$. By Theorem 6.1(i) we have

$$\left(\frac{b-\frac{cx}{dy}}{2}\right)^{\frac{p-1}{4}}\equiv(-1)^{\frac{a/2+b}{2}}(d/c)^n\left(\frac{a}{2}\right)^{\frac{p-1}{4}}\left(a^2+b^2\right)^{\frac{p-5}{8}}\frac{x}{y}\pmod p.$$

Substituting d by $-d$ and n by $1+(\frac{k}{p})-n$ we obtain

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

Hence applying (6.7) and (6.8) we have

$$\begin{aligned} U_{\frac{p-1}{4}}\big(b,-k^2\big) &\equiv \left(-\left(\frac{k}{p}\right)-1\right)(-1)^{\frac{a/2+b}{2}}(d/c)^{n+1}\left(\frac{a}{2}\right)^{\frac{p-1}{4}}\big(a^2+b^2\big)^{\frac{p-5}{8}} \\ &= \left(\left(\frac{k}{p}\right)+1\right)(-1)^{\frac{k-b}{2}}(d/c)^{n+1}k^{\frac{p-1}{4}}\big(b^2+4k^2\big)^{\frac{p-5}{8}} \pmod p \end{aligned}$$

and

$$\begin{aligned} V_{\frac{p-1}{4}}\big(b,-k^2\big) &\equiv \left(1-\left(\frac{k}{p}\right)\right)(-1)^{\frac{a/2+b}{2}}(d/c)^{n}\left(\frac{a}{2}\right)^{\frac{p-1}{4}}\big(a^2+b^2\big)^{\frac{p-5}{8}}\frac{x}{y} \\ &= \left(\left(\frac{k}{p}\right)-1\right)(-1)^{\frac{k-b}{2}}(d/c)^{n}\frac{x}{y}\cdot k^{\frac{p-1}{4}}\big(b^2+4k^2\big)^{\frac{p-5}{8}} \pmod p. \end{aligned}$$

If $2\nmid k$ and $4\mid y$, then $2\parallel a$ and $k_0=k$. By Theorem 6.1(i) we have

$$\left(\frac{b-\frac{cx}{dy}}{2}\right)^{\frac{p-1}{4}} \equiv (-1)^{\frac{b-1}{2}}(d/c)^{n-1}\left(\frac{a}{2}\right)^{\frac{p-1}{4}}\big(a^2+b^2\big)^{\frac{p-1}{8}} \pmod p.$$

Substituting d by $-d$ and n by $1+(\frac{k}{p})-n$ we obtain

$$\begin{aligned} \left(\frac{b+\frac{cx}{dy}}{2}\right)^{\frac{p-1}{4}} &\equiv (-1)^{\frac{b-1}{2}}\left(-\frac{d}{c}\right)^{(\frac{k}{p})-n}\left(\frac{a}{2}\right)^{\frac{p-1}{4}}\big(a^2+b^2\big)^{\frac{p-1}{8}} \\ &\equiv (-1)^{\frac{b-1}{2}}\left(\frac{k}{p}\right)(d/c)^{n-1}\left(\frac{a}{2}\right)^{\frac{p-1}{4}}\big(a^2+b^2\big)^{\frac{p-1}{8}} \pmod p. \end{aligned}$$

Hence, by (6.7), (6.8) and the above we have

$$\begin{aligned} U_{\frac{p-1}{4}}\big(b,-k^2\big) &\equiv \frac{1}{cx/(dy)}\left(\left(\frac{k}{p}\right)-1\right)(-1)^{\frac{b-1}{2}}(d/c)^{n-1}\left(\frac{a}{2}\right)^{\frac{p-1}{4}}\big(a^2+b^2\big)^{\frac{p-1}{8}} \\ &= \left(\left(\frac{k}{p}\right)-1\right)(-1)^{\frac{b-1}{2}}(d/c)^{n}\frac{y}{x}\cdot k^{\frac{p-1}{4}}\big(b^2+4k^2\big)^{\frac{p-1}{8}} \pmod p \end{aligned}$$

and

$$\begin{aligned} V_{\frac{p-1}{4}}\big(b,-k^2\big) &\equiv \left(\left(\frac{k}{p}\right)+1\right)(-1)^{\frac{b-1}{2}}(d/c)^{n-1}\left(\frac{a}{2}\right)^{\frac{p-1}{4}}\big(a^2+b^2\big)^{\frac{p-1}{8}} \\ &= \left(\left(\frac{k}{p}\right)+1\right)(-1)^{\frac{b-1}{2}}(d/c)^{n-1}k^{\frac{p-1}{4}}\big(b^2+4k^2\big)^{\frac{p-1}{8}} \pmod p. \end{aligned}$$

In a similar way one can prove the remaining results. So the theorem is proved. □

Theorem 6.3. *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 $b\in\mathbb{Z}$ and $2\nmid b$. Assume $p=x^2+(b^2+4)y^2$ with $x,y\in\mathbb{Z}$, $x=2^{\alpha}x_0$, $y=2^{\beta}y_0$ and $x_0\equiv y_0\equiv 1 \pmod 4$. Then*

$$U_{\frac{p-1}{4}}(b,-1)\equiv \begin{cases} 0 \pmod p & \textit{if } 4\mid xy, \\ \pm 2(-1)^{[\frac{p}{8}]}\delta(b,p)(x/y)^{\frac{p-5}{4}}\frac{d}{c} \pmod p & \textit{if } 4\nmid xy \textit{ and } (\frac{(2c+bd)/x}{b+2i})_4=\pm 1, \\ \mp 2(-1)^{[\frac{p}{8}]}\delta(b,p)(x/y)^{\frac{p-5}{4}} \pmod p & \textit{if } 4\nmid xy \textit{ and } (\frac{(2c+bd)/x}{b+2i})_4=\pm i \end{cases}$$

and

$$V_{\frac{p-1}{4}}(b,-1)\equiv\begin{cases}0 \pmod p & \text{if } 4\nmid xy,\\ \pm 2(-1)^{[\frac{p-5}{8}]}\delta'(b,p)(x/y)^{\frac{p-1}{4}}\frac{d}{c} \pmod p & \text{if } 4\mid xy \text{ and } \big(\frac{(2c+bd)/x}{b+2i}\big)_4=\pm 1,\\ \mp 2(-1)^{[\frac{p-5}{8}]}\delta'(b,p)(x/y)^{\frac{p-1}{4}} \pmod p & \text{if } 4\mid xy \text{ and } \big(\frac{(2c+bd)/x}{b+2i}\big)_4=\pm i,\end{cases}$$

where

$$\delta(b,p)=\begin{cases}(-1)^{\frac{b^2-1}{8}} & \text{if } p\equiv 1 \pmod 8,\\ (-1)^{\frac{b-1}{2}} & \text{if } p\equiv 5 \pmod 8)\end{cases}$$

and

$$\delta'(b,p)=\begin{cases}(-1)^{\frac{b-1}{2}} & \text{if } p\equiv 1 \pmod 8,\\ (-1)^{\frac{b^2-1}{8}} & \text{if } p\equiv 5 \pmod 8).\end{cases}$$

Proof. Suppose $(\frac{(2c+bd)/x}{b+2i})_4=i^n$. If $(\frac{(2c+bd)/x}{b+2i})_4=\pm 1$, then clearly $(d/c)^n\equiv\pm 1 \pmod p$. If $(\frac{(2c+bd)/x}{b+2i})_4=\pm i$, then $(d/c)^n\equiv\pm d/c \pmod p$. As $(x/y)^2\equiv -b^2-4 \pmod p$, we have $(b^2+4)^{[p/8]}\equiv(-1)^{[p/8]}(x/y)^{2[p/8]} \pmod p$. Thus taking $k=1$ in Theorem 6.2 we deduce the result. □

Corollary 6.4. *Let* $p\equiv 1,9 \pmod{20}$ *be a prime and hence* $p=c^2+d^2=x^2+5y^2$ *for some* $c,d,x,y\in\mathbb{Z}$. *Suppose* $c\equiv 1 \pmod 4$, $x=2^\alpha x_0$, $y=2^\beta y_0$ *and* $x_0\equiv y_0\equiv 1 \pmod 4$. *Then*

$$F_{\frac{p-1}{4}}\equiv\begin{cases}0 \pmod p & \text{if } 4\mid xy,\\ \mp 2(-1)^{[\frac{p}{8}]}(x/y)^{\frac{p-5}{4}} \pmod p & \text{if } 4\nmid xy \text{ and } x\equiv\pm c \pmod 5,\\ \pm 2(-1)^{[\frac{p}{8}]}(x/y)^{\frac{p-5}{4}}\frac{d}{c} \pmod p & \text{if } 4\nmid xy \text{ and } x\equiv\pm d \pmod 5\end{cases}$$

and

$$L_{\frac{p-1}{4}}\equiv\begin{cases}0 \pmod p & \text{if } 4\nmid xy,\\ \mp 2(-1)^{[\frac{p-5}{8}]}(x/y)^{\frac{p-1}{4}} \pmod p & \text{if } 4\mid xy \text{ and } x\equiv\pm c \pmod 5,\\ \pm 2(-1)^{[\frac{p-5}{8}]}(x/y)^{\frac{p-1}{4}}\frac{d}{c} \pmod p & \text{if } 4\mid xy \text{ and } x\equiv\pm d \pmod 5.\end{cases}$$

Proof. Putting $b=1$ in Theorem 6.3 and applying (6.5) we obtain the result. □

Corollary 6.5. *Let* $p\equiv 1,9,17,25,29,49 \pmod{52}$ *be a prime and hence* $p=c^2+d^2=x^2+13y^2$ *for some* $c,d,x,y\in\mathbb{Z}$. *Suppose* $c\equiv 1 \pmod 4$, $x=2^\alpha x_0$, $y=2^\beta y_0$ *and* $x_0\equiv y_0\equiv 1 \pmod 4$. *Then*

$$U_{\frac{p-1}{4}}(3,-1)\equiv\begin{cases}0 \pmod p & \text{if } 4\mid xy,\\ \mp 2(-1)^{[\frac{p}{8}]}(x/y)^{\frac{p-5}{4}}\frac{d}{c} \pmod p & \text{if } 4\nmid xy \text{ and } \frac{2c+3d}{x}\equiv\pm 1,\pm 3,\pm 9 \pmod{13},\\ \mp 2(-1)^{[\frac{p}{8}]}(x/y)^{\frac{p-5}{4}} \pmod p & \text{if } 4\nmid xy \text{ and } \frac{2c+3d}{x}\equiv\pm 2,\pm 5,\pm 6 \pmod{13}\end{cases}$$

and

$$V_{\frac{p-1}{4}}(3,-1)\equiv\begin{cases}0 \pmod p & \text{if } 4\nmid xy,\\ \mp 2(-1)^{[\frac{p-5}{8}]}(x/y)^{\frac{p-1}{4}}\frac{d}{c} \pmod p & \text{if } 4\mid xy \text{ and } \frac{2c+3d}{x}\equiv\pm 1,\pm 3,\pm 9 \pmod{13},\\ \mp 2(-1)^{[\frac{p-5}{8}]}(x/y)^{\frac{p-1}{4}} \pmod p & \text{if } 4\mid xy \text{ and } \frac{2c+3d}{x}\equiv\pm 2,\pm 5,\pm 6 \pmod{13}.\end{cases}$$

Proof. Putting $b=3$ in Theorem 6.3 and applying (6.6) we obtain the result. □

Theorem 6.4. *Let $p \equiv 1 \pmod 8$ be a prime and $p = c^2 + d^2$ with $c, d \in \mathbb{Z}$ and $c \equiv 1 \pmod 4$. Let $b \in \mathbb{Z}$, $2 \nmid b$, $p \neq b^2 + 4$ and $p = x^2 + (b^2 + 4)y^2$ with $x, y \in \mathbb{Z}$. Then $p \mid U_{\frac{p-1}{8}}(b, -1)$ if and only if $2 \nmid x$ and*

$$(-b^2-4)^{\frac{p-1}{8}} \equiv \begin{cases} \pm(-1)^{\frac{b-1}{2}} \pmod p & \text{if } \left(\frac{(2c+bd)/x}{b+2i}\right)_4 = \pm i, \\ \pm(-1)^{\frac{b-1}{2}} \frac{d}{c} \pmod p & \text{if } \left(\frac{(2c+bd)/x}{b+2i}\right)_4 = \pm 1, \end{cases}$$

where x is chosen so that $x \equiv 1 \pmod 4$.

Proof. If $p \mid U_{\frac{p-1}{8}}(b, -1)$, then $U_{\frac{p-1}{4}}(b, -1) = U_{\frac{p-1}{8}}(b, -1)V_{\frac{p-1}{8}}(b, -1) \equiv 0 \pmod p$ and so $4 \mid xy$ by Theorem 6.3. As $p \equiv 1 \pmod 8$, we must have $4 \nmid x$ and so $4 \mid y$. Now assume $4 \mid y$ and $x \equiv 1 \pmod 4$. From (1.5) and Theorem 6.3 we see that

$$\begin{aligned} p \mid U_{\frac{p-1}{8}}(b,-1) &\iff V_{\frac{p-1}{4}}(b,-1) \equiv 2(-1)^{\frac{p-1}{8}} \pmod p \\ &\iff \begin{cases} \pm(-1)^{\frac{b-1}{2}}(x/y)^{\frac{p-1}{4}} \equiv 1 \pmod p & \text{if } \left(\frac{(2c+bd)/x}{b+2i}\right)_4 = \pm i, \\ \mp(-1)^{\frac{b-1}{2}}(x/y)^{\frac{p-1}{4}} \frac{d}{c} \equiv 1 \pmod p & \text{if } \left(\frac{(2c+bd)/x}{b+2i}\right)_4 = \pm 1. \end{cases} \end{aligned}$$

As $(x/y)^2 \equiv -b^2 - 4 \pmod p$ we have $(x/y)^{\frac{p-1}{4}} \equiv (-b^2-4)^{\frac{p-1}{8}} \pmod p$. Thus the result follows. □

Putting $b = 1$ in Theorem 6.4 and then applying (6.5) we deduce the following result.

Corollary 6.6. *Let $p \equiv 1, 9 \pmod{40}$ be a prime and hence $p = c^2 + d^2 = x^2 + 5y^2$ for some $c, d, x, y \in \mathbb{Z}$. Suppose $c \equiv 1 \pmod 4$. Then*

$$p \mid F_{\frac{p-1}{8}} \iff 2 \nmid x \quad \text{and} \quad (-5)^{\frac{p-1}{8}} \equiv \begin{cases} \pm 1 \pmod p & \text{if } x \equiv \pm c \pmod 5, \\ \pm\frac{d}{c} \pmod p & \text{if } x \equiv \pm d \pmod 5, \end{cases}$$

where x is chosen so that $x \equiv 1 \pmod 4$.

Remark 6.1. Under the condition in Corollary 6.6, in 1974 E. Lehmer [L2] conjectured that if $p \equiv 1 \pmod{16}$, then

$$p \mid F_{\frac{p-1}{8}} \iff 4 \mid y \quad \text{and} \quad (-1)^{\frac{d}{4}} = (-1)^{\frac{y}{4}}.$$

We also note that if $p \equiv 1 \pmod 8$ and $p \not\equiv 1, 9 \pmod{40}$, then $p \nmid F_{\frac{p-1}{8}}$.

Putting $b = 3$ in Theorem 6.4 and applying (6.6) we have:

Corollary 6.7. *Let $p \equiv 1, 9, 17, 25, 49, 81 \pmod{104}$ be a prime and hence $p = c^2 + d^2 = x^2 + 13y^2$ for some $c, d, x, y \in \mathbb{Z}$. Suppose $c \equiv 1 \pmod 4$. Then $p \mid U_{\frac{p-1}{8}}(3, -1)$ if and only if $2 \nmid x$ and*

$$(-13)^{\frac{p-1}{8}} \equiv \begin{cases} \pm 1 \pmod p & \text{if } \frac{2c+3d}{x} \equiv \pm 2, \pm 5, \pm 6 \pmod{13}, \\ \pm\frac{c}{d} \pmod p & \text{if } \frac{2c+3d}{x} \equiv \pm 1, \pm 3, \pm 9 \pmod{13}, \end{cases}$$

where x is chosen so that $x \equiv 1 \pmod 4$.

Theorem 6.5. *Let $p \equiv 1, 9 \pmod{40}$ be a prime and hence $p = C^2 + 2D^2 = x^2 + 5y^2$ for some $C, D, x, y \in \mathbb{Z}$. Suppose $C \equiv 1 \pmod 4$, $x = 2^\alpha x_0$, $y = 2^\beta y_0$ and $x_0 \equiv y_0 \equiv 1 \pmod 4$.*

(i) *If* $2 \mid x$ *and* $x \equiv \pm C, \pm 3C \pmod 5$, *then*

$$p \mid L_{\frac{p-1}{4}} \quad \textit{and} \quad F_{\frac{p-1}{4}} \equiv \pm 2\left(\frac{x}{5}\right)\frac{y}{x} \pmod p.$$

(ii) *If* $2 \nmid x$ *and* $x \equiv \pm C, \pm 3C \pmod 5$, *then*

$$p \mid F_{\frac{p-1}{4}} \quad \textit{and} \quad L_{\frac{p-1}{4}} \equiv \pm 2\left(\frac{x}{5}\right) \pmod p.$$

Proof. Clearly $5 \nmid xC$. Thus $x \equiv \pm C$ or $\pm 3C \pmod 5$. Suppose $p = c^2 + d^2$ with $c, d \in \mathbb{Z}$ and $c \equiv 1 \pmod 4$. As $(\frac{5}{p}) = 1$, it is known that (see for example [S4, Theorem 2.2 and Example 2.1]) $5 \mid cd$ and

$$5^{\frac{p-1}{4}} \equiv \begin{cases} 1 \pmod p & \text{if } 5 \mid d, \\ -1 \pmod p & \text{if } 5 \mid c. \end{cases} \tag{6.9}$$

On the other hand, by Theorem 2.3 or [BEW, Corollary 8.3.4] we have

$$5^{\frac{p-1}{4}} \equiv -(-1)^x\left(\frac{x}{5}\right) \pmod p. \tag{6.10}$$

If $5^{\frac{p-1}{4}} \equiv -1 \pmod p$, by [HW2, Theorem 3] we have

$$5^{\frac{p-1}{8}} \equiv \begin{cases} \frac{c}{d} \pmod p & \text{if } d \equiv C, 3C \pmod 5, \\ -\frac{c}{d} \pmod p & \text{if } d \equiv -C, -3C \pmod 5. \end{cases} \tag{6.11}$$

If $5^{\frac{p-1}{4}} \equiv 1 \pmod p$, by [E, Theorem 5.1 or Corollary 5.3] we have

$$5^{\frac{p-1}{8}} \equiv \begin{cases} 1 \pmod p & \text{if } c \equiv C, 3C \pmod 5, \\ -1 \pmod p & \text{if } c \equiv -C, -3C \pmod 5. \end{cases} \tag{6.12}$$

Suppose $x \equiv \varepsilon C$ or $3\varepsilon C \pmod 5$, where $\varepsilon \in \{1, -1\}$. We first consider (i). As $p \equiv 1 \pmod 8$ and $2 \mid x$ we must have $2 \nmid y$ and $2 \parallel x$. Thus $p \mid L_{\frac{p-1}{4}}$ by Corollary 6.4. If $p \equiv 1 \pmod{40}$, then $x \equiv \pm 1 \pmod 5$. By (6.9) and (6.10) we have $5^{\frac{p-1}{4}} \equiv -1 \pmod p$ and $5 \mid c$. We may choose the sign of d so that $d \equiv x \equiv \varepsilon C, 3\varepsilon C \pmod 5$. Then $5^{\frac{p-1}{8}} \equiv \varepsilon c/d \pmod p$ by (6.11). By Corollary 6.4 we have

$$\begin{aligned} F_{\frac{p-1}{4}} &\equiv 2(-1)^{\frac{p-1}{8}}(x/y)^{\frac{p-5}{4}}\frac{d}{c} = 2(-1)^{\frac{p-1}{8}}(x/y)^{\frac{p-1}{4}}\frac{dy}{cx} \\ &\equiv 2 \cdot 5^{\frac{p-1}{8}}\frac{dy}{cx} \equiv 2\varepsilon\frac{c}{d} \cdot \frac{dy}{cx} = 2\varepsilon\frac{y}{x} \pmod p. \end{aligned}$$

So (i) is true in the case $p \equiv 1 \pmod{40}$. Now assume $p \equiv 9 \pmod{40}$. Then $x \equiv \pm 2 \pmod 5$. By (6.9) and (6.10) we have $5^{\frac{p-1}{4}} \equiv 1 \pmod p$, $5 \mid d$ and so $x \equiv \pm c \pmod 5$. If $x \equiv \pm c \pmod 5$, then $c \equiv \pm\varepsilon C, \pm 3\varepsilon C \pmod 5$. Thus, by (6.12) we have $5^{\frac{p-1}{8}} \equiv \pm\varepsilon \pmod p$. Hence applying Corollary 6.4 we have

$$F_{\frac{p-1}{4}} \equiv \mp 2(-1)^{\frac{p-1}{8}}(x/y)^{\frac{p-5}{4}} \equiv \mp 2 \cdot 5^{\frac{p-1}{8}}\frac{y}{x} \equiv -2\varepsilon\frac{y}{x} \pmod p.$$

This proves (i).

Now we consider (ii). Suppose $2 \nmid x$. Then $4 \mid y$ as $p \equiv 1 \pmod 8$. Thus $p \mid F_{\frac{p-1}{4}}$ by Corollary 6.4. If $p \equiv 1 \pmod{40}$, we have $x \equiv \pm 1 \pmod 5$. By (6.9) and (6.10) we have $5^{\frac{p-1}{4}} \equiv 1 \pmod p$, $5 \mid d$ and so $x \equiv \pm c \pmod 5$. When $x \equiv \pm c \pmod 5$, by (6.12) we have $5^{\frac{p-1}{8}} \equiv \pm \varepsilon \pmod p$. Thus, by Corollary 6.4 we have

$$L_{\frac{p-1}{4}} \equiv \pm 2(-1)^{\frac{p-1}{8}}(x/y)^{\frac{p-1}{4}} \equiv \pm 2 \cdot 5^{\frac{p-1}{8}} \equiv 2\varepsilon \pmod p.$$

If $p \equiv 9 \pmod{40}$, then $x \equiv \pm 2 \pmod 5$. By (6.9) and (6.10) we have $5^{\frac{p-1}{4}} \equiv -1 \pmod p$, $5 \mid c$ and so $x \equiv \pm d \pmod 5$. If $x \equiv \pm d \pmod 5$, by (6.11) we have $5^{\frac{p-1}{8}} \equiv \pm \varepsilon c/d \pmod p$. Thus, by Corollary 6.4 we have

$$L_{\frac{p-1}{4}} \equiv \pm 2(-1)^{\frac{p-1}{8}-1}(x/y)^{\frac{p-1}{4}}\frac{d}{c} \equiv \mp 2 \cdot 5^{\frac{p-1}{8}}\frac{d}{c} \equiv -2\varepsilon \pmod p.$$

Hence (ii) holds and the theorem is proved. □

Corollary 6.8. *Let $p \equiv 1, 9 \pmod{40}$ be a prime and hence $p = C^2 + 2D^2 = x^2 + 5y^2$ for some $C, D, x, y \in \mathbb{Z}$. Suppose $C \equiv 1 \pmod 4$, $x = 2^\alpha x_0$, $y = 2^\beta y_0$ and $x_0 \equiv y_0 \equiv 1 \pmod 4$.*

(i) *If $2 \mid x$ and $x \equiv \pm C, \pm 3C \pmod 5$, then*

$$\left(\frac{1+\sqrt{5}}{2}\right)^{\frac{p-1}{4}} \equiv -\left(\frac{1-\sqrt{5}}{2}\right)^{\frac{p-1}{4}} \equiv \pm\left(\frac{x}{5}\right)\frac{y}{x}\sqrt{5} \pmod p.$$

(ii) *If $2 \nmid x$ and $x \equiv \pm C, \pm 3C \pmod 5$, then*

$$\left(\frac{1+\sqrt{5}}{2}\right)^{\frac{p-1}{4}} \equiv \left(\frac{1-\sqrt{5}}{2}\right)^{\frac{p-1}{4}} \equiv \pm\left(\frac{x}{5}\right) \pmod p.$$

Proof. From (1.3) and (1.4) we know that

$$F_n = \frac{1}{\sqrt{5}}\left\{\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n\right\}$$

and

$$L_n = \left(\frac{1+\sqrt{5}}{2}\right)^n + \left(\frac{1-\sqrt{5}}{2}\right)^n.$$

Thus

$$\left(\frac{1\pm\sqrt{5}}{2}\right)^n = \frac{L_n \pm \sqrt{5}F_n}{2}.$$

Now applying Theorem 6.5 we obtain the result. □

Corollary 6.9. *Let $p \equiv 1 \pmod 8$ be a prime and hence $p = C^2 + 2D^2$ with $C, D \in \mathbb{Z}$ and $C \equiv 1 \pmod 4$. Then $p \mid F_{\frac{p-1}{8}}$ if and only if $p = x^2 + 5y^2$ with $x, y \in \mathbb{Z}$, $x \equiv 1 \pmod 4$ and*

$$x \equiv \begin{cases} C, 3C \pmod 5 & \text{if } p \equiv 1, 9 \pmod{80}, \\ -C, -3C \pmod 5 & \text{if } p \equiv 41, 49 \pmod{80}. \end{cases}$$

Proof. It is well known that (see for example [SS, p. 372]) $F_{p-1} \equiv \frac{1}{2}(1-(\frac{p}{5}))\pmod p$ and $F_n \mid F_{mn}$ for any positive integers m and n. Thus, if $p \mid F_{\frac{p-1}{8}}$, then $p \mid F_{p-1}$ and so $(\frac{p}{5})=1$. Hence $p\equiv 1,9 \pmod{40}$ and so $p=x^2+5y^2$ for some $x,y\in\mathbb{Z}$. We note that $p\equiv 1\pmod{40}$ implies $x\equiv \pm 1\pmod 5$, and $p\equiv 9\pmod{40}$ implies $x\equiv\pm 2\pmod 5$. As

$$\begin{aligned} p \mid F_{\frac{p-1}{8}} &\iff \left(\frac{1+\sqrt5}{2}\right)^{\frac{p-1}{8}} \equiv \left(\frac{1-\sqrt5}{2}\right)^{\frac{p-1}{8}} \pmod p \\ &\iff \left(\frac{1+\sqrt5}{2}\right)^{\frac{p-1}{4}} \equiv (-1)^{\frac{p-1}{8}} \pmod p, \end{aligned}$$

applying Corollary 6.8 we deduce the result. □

Corollary 6.10. *Let $p\equiv 1,9\pmod{40}$ be a prime and hence $p=C^2+2D^2=x^2+5y^2$ for some $C,D,x,y\in\mathbb{Z}$. Suppose $C\equiv 1\pmod 4$, $x=2^\alpha x_0$, $y=2^\beta y_0$ and $x_0\equiv y_0\equiv 1\pmod 4$.*

(i) *If $2\mid x$ and $x\equiv\pm C,\pm 3C\pmod 5$, then*

$$U_{\frac{p-1}{4}}(4,-1)=\frac12 F_{\frac{3(p-1)}{4}}\equiv \mp\left(\frac{x}{5}\right)\frac{y}{x}\pmod p\quad \textit{and}\quad p\mid V_{\frac{p-1}{4}}(4,-1).$$

(ii) *If $2\nmid x$ and $x\equiv\pm C,\pm 3C\pmod 5$, then*

$$p\mid U_{\frac{p-1}{4}}(4,-1)\quad \textit{and}\quad V_{\frac{p-1}{4}}(4,-1)=L_{\frac{3(p-1)}{4}}\equiv \pm 2\left(\frac{x}{5}\right)\pmod p.$$

(iii) $p\mid U_{\frac{p-1}{8}}(4,-1)$ *if and only if $x\equiv 1\pmod 4$ and*

$$x\equiv\begin{cases} C, 3C \pmod 5 & \textit{if } p\equiv 1,9 \pmod{80},\\ -C,-3C\pmod 5 & \textit{if } p\equiv 41,49\pmod{80}.\end{cases}$$

Proof. Observe that $2\pm\sqrt5=(\frac{1\pm\sqrt5}{2})^3$. From (1.3) and (1.4) we see that

$$U_{\frac{p-1}{4}}(4,-1)=\frac{1}{2\sqrt5}\left\{\left(\frac{1+\sqrt5}{2}\right)^{\frac{3(p-1)}{4}}-\left(\frac{1-\sqrt5}{2}\right)^{\frac{3(p-1)}{4}}\right\}=\frac12 F_{\frac{3(p-1)}{4}}$$

and

$$V_{\frac{p-1}{4}}(4,-1)=\left(\frac{1+\sqrt5}{2}\right)^{\frac{3(p-1)}{4}}+\left(\frac{1-\sqrt5}{2}\right)^{\frac{3(p-1)}{4}}=L_{\frac{3(p-1)}{4}}.$$

Now applying the above and Corollary 6.8 we obtain (i) and (ii). Suppose $x\equiv\pm C,\pm 3C\pmod 5$. By (i), (ii) and (1.5) we have

$$\begin{aligned} p\mid U_{\frac{p-1}{8}}(4,-1) &\iff V_{\frac{p-1}{4}}(4,-1)\equiv \pm 2\left(\frac{x}{5}\right)\equiv 2(-1)^{\frac{p-1}{8}}\pmod p\\ &\iff 2\nmid x\quad\text{and}\quad (-1)^{\frac{p-1}{8}}\left(\frac{x}{5}\right)=\pm 1. \end{aligned}$$

As $(-1)^{\frac{p-1}{8}}(\frac{x}{5}) = 1$ if and only if $p \equiv 1, 9 \pmod{80}$, we see that (iii) holds and so the corollary is proved. □

7. Congruences for $U_{\frac{p-1}{4}}(4a, -k^2)$ and $V_{\frac{p-1}{4}}(4a, -k^2) \pmod p$

Theorem 7.1. *Let $B, k \in \mathbb{Z}$, $2 \mid B$ and $(B, k) = 1$. Let $p \equiv 1 \pmod 4$ be a prime such that $p = c^2 + d^2 = x^2 + (B^2 + k^2)y^2$ with $c, d, x, y \in \mathbb{Z}$, $c \equiv 1 \pmod 4$ and $B^2 + k^2 \neq p$. Suppose $x = 2^\alpha x_0$, $y = 2^\beta y_0$, $x_0 \equiv y_0 \equiv 1 \pmod 4$ and $(\frac{x-Byi}{k})_4(\frac{(kd-Bc)/x}{k-Bi})_4 = i^m$.*

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

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

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

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

Proof. Suppose $(\frac{kd-Bc}{k-Bi})_4 = i^s$. Then $(\frac{kd-Bc}{k+Bi})_4 = i^{-s}$. By Corollary 4.1 we have

$$\left(-B - k\frac{c}{d}\right)^{\frac{p-1}{4}} \equiv \begin{cases} (-1)^{\frac{k+1}{2}\cdot\frac{d}{2}}(c/d)^{\frac{p-1}{4}+s} \pmod p & \text{if } 4 \mid B, \\ (-1)^{\frac{k-1}{2}(\frac{d}{2}+1)}(c/d)^{\frac{p-1}{4}-1+s} \pmod p & \text{if } 2 \parallel B. \end{cases}$$

Note that $(c/d)^2 \equiv -1 \pmod p$ and $(-1)^{\frac{p-1}{4}} = (-1)^{\frac{d}{2}}$. We then have

$$(-B - kc/d)^{-\frac{p-1}{4}} \equiv \begin{cases} (-1)^{\frac{p-1}{8}}(c/d)^{-s} \pmod p & \text{if } 8 \mid p-1 \text{ and } 4 \mid B, \\ (-1)^{\frac{k-1}{2}+\frac{p-5}{8}}(c/d)^{1-s} \pmod p & \text{if } 8 \mid p-5 \text{ and } 4 \mid B, \\ (-1)^{\frac{k-1}{2}+\frac{p-1}{8}}(c/d)^{1-s} \pmod p & \text{if } 8 \mid p-1 \text{ and } 2 \parallel B, \\ (-1)^{\frac{p-5}{8}}(c/d)^{-s} \pmod p & \text{if } 8 \mid p-5 \text{ and } 2 \parallel B. \end{cases} \tag{7.1}$$

From (6.1) we see that

$$\left(-B - k\frac{c}{d}\right)\left(B - \frac{cx}{dy}\right) \equiv \frac{1}{2}\left(\frac{x}{y} - k + B\frac{c}{d}\right)^2 \pmod p.$$

Thus

$$\left(B - \frac{cx}{dy}\right)^{\frac{p-1}{4}} \equiv \left(\frac{x}{y} - k + B\frac{c}{d}\right)^{\frac{p-1}{2}} \cdot 2^{-\frac{p-1}{4}}\left(-B - k\frac{c}{d}\right)^{-\frac{p-1}{4}} \pmod p. \tag{7.2}$$

As $p \ne B^2 + k^2$ we see that $p \nmid kxy$. By Theorem 5.1(ii) we have

$$\left(\frac{x/y - k + Bi}{p}\right)_4 = \left(\frac{x - ky + Byi}{p}\right)_4$$
$$= \begin{cases} (\frac{x+Byi}{k})_4(\frac{x}{-k+Bi})_4 & \text{if } 2 \mid y, \\ i^{-\frac{B}{2}}(\frac{x+Byi}{k})_4(\frac{x}{-k+Bi})_4 & \text{if } 2 \nmid y. \end{cases}$$

As

$$\left(\frac{x + Byi}{k}\right)_4 \left(\frac{x}{-k + Bi}\right)_4 \cdot \left(\frac{x - Byi}{k}\right)_4 \left(\frac{(kd - Bc)/x}{k - Bi}\right)_4$$
$$= \left(\frac{x^2 + B^2y^2}{k}\right)_4 \left(\frac{kd - Bc}{k - Bi}\right)_4 = \left(\frac{p - k^2y^2}{k}\right)_4 i^s = i^s,$$

by the above we have

$$\left(\frac{x/y - k + Bi}{p}\right)_4 = \begin{cases} i^{s-m} & \text{if } 2 \mid y, \\ i^{s-m-\frac{B}{2}} & \text{if } 2 \nmid y. \end{cases}$$

This together with Lemma 6.1 yields

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

Combining this with (7.1) and (7.2) we obtain the result. □

Theorem 7.2. *Let $b, k \in \mathbb{Z}$, $4 \mid b$ and $(b, k) = 1$. Let $p \equiv 1 \pmod 4$ be a prime such that $p = c^2 + d^2 = x^2 + (b^2/4 + k^2)y^2$ with $c, d, x, y \in \mathbb{Z}$, $c \equiv 1 \pmod 4$ and $b^2/4 + k^2 \ne p$. Suppose $x = 2^\alpha x_0$, $y = 2^\beta y_0$, $x_0 \equiv y_0 \equiv 1 \pmod 4$ and $(\frac{x-\frac{b}{2}yi}{k})_4(\frac{(kd-\frac{b}{2}c)/x}{k-\frac{b}{2}i})_4 = i^m$.*

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

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

and

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

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

$$U_{\frac{p-1}{4}}(b, -k^2) \equiv \begin{cases} \frac{1+(\frac{k}{p})}{2}(-1)^{\frac{k-1}{2}+\frac{b}{8}y}k^{\frac{p-1}{4}}(b^2/4+k^2)^{\frac{p-5}{8}}(d/c)^m \pmod p & \text{if } 8 \mid b, \\ \frac{1+(\frac{k}{p})}{2}k^{\frac{p-1}{4}}(b^2/4+k^2)^{\frac{p-5}{8}}(d/c)^{m+1} \pmod p & \text{if } 8 \mid b-4 \text{ and } 2 \mid y, \\ \frac{(\frac{k}{p})-1}{2}(-1)^{\frac{b-4}{8}}k^{\frac{p-1}{4}}(b^2/4+k^2)^{\frac{p-5}{8}}(d/c)^m \pmod p & \text{if } 8 \mid b-4 \text{ and } 2 \nmid y \end{cases}$$

and

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

Proof. Set $B = b/2$. Then B is even. By (1.3) and (1.4) we have

$$\begin{aligned} U_{\frac{p-1}{4}}(b, -k^2) &= \frac{1}{2\sqrt{B^2+k^2}}\left\{\left(B+\sqrt{B^2+k^2}\right)^{\frac{p-1}{4}} - \left(B-\sqrt{B^2+k^2}\right)^{\frac{p-1}{4}}\right\} \\ &\equiv \frac{dy}{2cx}\left\{\left(B+\frac{cx}{dy}\right)^{\frac{p-1}{4}} - \left(B-\frac{cx}{dy}\right)^{\frac{p-1}{4}}\right\} \pmod p \end{aligned} \tag{7.3}$$

and

$$\begin{aligned} V_{\frac{p-1}{4}}(b, -k^2) &= \left(B+\sqrt{B^2+k^2}\right)^{\frac{p-1}{4}} + \left(B-\sqrt{B^2+k^2}\right)^{\frac{p-1}{4}} \\ &\equiv \left(B+\frac{cx}{dy}\right)^{\frac{p-1}{4}} + \left(B-\frac{cx}{dy}\right)^{\frac{p-1}{4}} \pmod p. \end{aligned} \tag{7.4}$$

Applying Proposition 2.4 we have

$$\begin{aligned} \left(\frac{x-Byi}{k}\right)_4\left(\frac{(-kd-Bc)/x}{k-Bi}\right)_4 \cdot i^m &= \left(\frac{x-Byi}{k}\right)_4^2\left(\frac{(-Bc+kd)(-Bc-kd)/x^2}{k-Bi}\right)_4 \\ &= \left(\frac{x^2+B^2y^2}{k}\right)\left(\frac{B^2c^2-k^2d^2}{k-Bi}\right)_4\left(\frac{x^2}{k-Bi}\right)_4^{-1} \\ &= \left(\frac{p-k^2y^2}{k}\right)\left(\frac{-k^2(c^2+d^2)}{k-Bi}\right)_4\left(\frac{x^2}{k-Bi}\right)_4^{-1} \\ &= \left(\frac{p}{k}\right)(-1)^{\frac{B}{2}}\left(\frac{k^2}{k-Bi}\right)_4\left(\frac{x^2+(B^2+k^2)y^2}{k-Bi}\right)_4\left(\frac{x^2}{k-Bi}\right)_4^{-1} \\ &= \left(\frac{k}{p}\right)(-1)^{\frac{B}{2}}\left(\frac{k-Bi}{k}\right)_4^2\left(\frac{x^2}{k-Bi}\right)_4\left(\frac{x^2}{k-Bi}\right)_4^{-1} \\ &= (-1)^{\frac{B}{2}}\left(\frac{k}{p}\right), \end{aligned}$$

thus

$$\left(\frac{x-Byi}{k}\right)_4\left(\frac{(k(-d)-Bc)/x}{k-Bi}\right)_4=(-1)^{\frac{B}{2}}\left(\frac{k}{p}\right)i^{-m}=i^{B+(\frac{k}{p})-1-m}.$$

Set $d'=-d$ and $m'=B+(\frac{k}{p})-1-m$. Then $(\frac{x-Byi}{k})_4(\frac{(kd'-Bc)/x}{k-Bi})_4=i^{m'}$. We also have

$$(d'/c)^{m'}=(-d/c)^{B+(\frac{k}{p})-1-m}\equiv(-1)^{\frac{B}{2}}\left(\frac{k}{p}\right)(d/c)^m \pmod p$$

and

$$(d'/c)^{m'-1}\equiv(-1)^{\frac{B}{2}}\left(\frac{k}{p}\right)(d/c)^m(-d/c)^{-1}=-(-1)^{\frac{B}{2}}\left(\frac{k}{p}\right)(d/c)^{m-1} \pmod p.$$

Now substituting d,m by d',m' in Theorem 7.1 we see that if $p\equiv 1\pmod 8$, then

$$\left(B+\frac{cx}{dy}\right)^{\frac{p-1}{4}}\equiv\begin{cases}(\frac{k}{p})k^{\frac{p-1}{4}}(B^2+k^2)^{\frac{p-1}{8}}(d/c)^m \pmod p & \text{if } 4\mid B \text{ and } 2\mid y,\\ (\frac{k}{p})(-1)^{\frac{B}{4}}k^{\frac{p-1}{4}}(B^2+k^2)^{\frac{p-1}{8}}(d/c)^m \pmod p & \text{if } 4\mid B \text{ and } 2\nmid y,\\ (\frac{k}{p})(-1)^{\frac{k-1}{2}}k^{\frac{p-1}{4}}(B^2+k^2)^{\frac{p-1}{8}}(d/c)^{m-1} \pmod p & \text{if } 2\parallel B \text{ and } 2\mid y,\\ -(\frac{k}{p})(-1)^{\frac{k-B/2}{2}}k^{\frac{p-1}{4}}(B^2+k^2)^{\frac{p-1}{8}}(d/c)^m \pmod p & \text{if } 2\parallel B \text{ and } 2\nmid y;\end{cases}$$

if $p\equiv 5\pmod 8$, then

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

This together with (7.3), (7.4) and Theorem 7.1 yields the result. □

Putting $b=4a$ and $k=1$ in Theorem 7.2 we have the following result.

Theorem 7.3. *Let $a\in\mathbb{Z}$. 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 $4a^2+1\neq p$. Suppose $x=2^\alpha x_0,\ y=2^\beta y_0$ and $x_0\equiv y_0\equiv 1\pmod 4$.*

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

$$U_{\frac{p-1}{4}}(4a,-1)\equiv\begin{cases}\pm(-1)^{\frac{a+1}{2}}(4a^2+1)^{\frac{p-1}{8}}\frac{dy}{cx} \pmod p & \text{if } 2\nmid ay \text{ and } (\frac{(d-2ac)/x}{1-2ai})_4=\pm 1,\\ \pm(-1)^{\frac{a-1}{2}}(4a^2+1)^{\frac{p-1}{8}}\frac{y}{x} \pmod p & \text{if } 2\nmid ay \text{ and } (\frac{(d-2ac)/x}{1-2ai})_4=\pm i,\\ 0 \pmod p & \text{if } 2\mid ay\end{cases}$$

and

$$V_{\frac{p-1}{4}}(4a,-1)\equiv\begin{cases}\pm 2(-1)^{\frac{a}{2}y}(4a^2+1)^{\frac{p-1}{8}}\pmod p & \text{if } 2\mid a \text{ and } \left(\frac{(d-2ac)/x}{1-2ai}\right)_4=\pm 1,\\ \pm 2(-1)^{\frac{a}{2}y}(4a^2+1)^{\frac{p-1}{8}}\frac{d}{c}\pmod p & \text{if } 2\mid a \text{ and } \left(\frac{(d-2ac)/x}{1-2ai}\right)_4=\pm i,\\ \mp 2(4a^2+1)^{\frac{p-1}{8}}\frac{d}{c}\pmod p & \text{if } 2\nmid a,\ 2\mid y \text{ and } \left(\frac{(d-2ac)/x}{1-2ai}\right)_4=\pm 1,\\ \pm 2(4a^2+1)^{\frac{p-1}{8}}\pmod p & \text{if } 2\nmid a,\ 2\mid y \text{ and } \left(\frac{(d-2ac)/x}{1-2ai}\right)_4=\pm i,\\ 0\pmod p & \text{if } 2\nmid ay.\end{cases}$$

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

$$U_{\frac{p-1}{4}}(4a,-1)\equiv\begin{cases}\pm(-1)^{\frac{a}{2}y}(4a^2+1)^{\frac{p-5}{8}}\pmod p & \text{if } 2\mid a \text{ and } \left(\frac{(d-2ac)/x}{1-2ai}\right)_4=\pm 1,\\ \pm(-1)^{\frac{a}{2}y}(4a^2+1)^{\frac{p-5}{8}}\frac{d}{c}\pmod p & \text{if } 2\mid a \text{ and } \left(\frac{(d-2ac)/x}{1-2ai}\right)_4=\pm i,\\ \pm(4a^2+1)^{\frac{p-5}{8}}\frac{d}{c}\pmod p & \text{if } 2\nmid a,\ 2\mid y \text{ and } \left(\frac{(d-2ac)/x}{1-2ai}\right)_4=\pm 1,\\ \mp(4a^2+1)^{\frac{p-5}{8}}\pmod p & \text{if } 2\nmid a,\ 2\mid y \text{ and } \left(\frac{(d-2ac)/x}{1-2ai}\right)_4=\pm i,\\ 0\pmod p & \text{if } 2\nmid ay\end{cases}$$

and

$$V_{\frac{p-1}{4}}(4a,-1)\equiv\begin{cases}0\pmod p & \text{if } 2\mid ay,\\ \pm 2(-1)^{\frac{a+1}{2}}(4a^2+1)^{\frac{p-5}{8}}\frac{dx}{cy}\pmod p & \text{if } 2\nmid ay \text{ and } \left(\frac{(d-2ac)/x}{1-2ai}\right)_4=\pm 1,\\ \pm 2(-1)^{\frac{a-1}{2}}(4a^2+1)^{\frac{p-5}{8}}\frac{x}{y}\pmod p & \text{if } 2\nmid ay \text{ and } \left(\frac{(d-2ac)/x}{1-2ai}\right)_4=\pm i.\end{cases}$$

Corollary 7.1. *Let* p *be a prime such that* $p\equiv 1, 9, 21, 25, 33, 41, 49, 53, 65, 73, 77, 81, 85, 101, 121, 137, 141, 145 \pmod{148}$ *and hence* $p=c^2+d^2=x^2+37y^2$ *for some* $c, d, x, y\in\mathbb{Z}$. *Suppose* $c\equiv 1\pmod 4$, $x=2^{\alpha}x_0$, $y=2^{\beta}y_0$ *and* $x_0\equiv y_0\equiv 1\pmod 4$.

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

$$U_{\frac{p-1}{4}}(12,-1)\equiv\begin{cases}\pm 37^{\frac{p-1}{8}}\frac{dy}{cx}\pmod p & \text{if } 2\nmid y \text{ and } \frac{d-6c}{x}\equiv\pm 1,\pm 7,\pm 9,\pm 10,\\ & \quad\pm 12,\pm 16,\pm 26,\pm 33,\pm 34\pmod{37},\\ \mp 37^{\frac{p-1}{8}}\frac{y}{x}\pmod p & \text{if } 2\nmid y \text{ and } \frac{d-6c}{x}\equiv\pm 2,\pm 14,\pm 15,\pm 18,\\ & \quad\pm 20,\pm 24,\pm 29,\pm 31,\pm 32\pmod{37},\\ 0\pmod p & \text{if } 2\mid y\end{cases}$$

and

$$V_{\frac{p-1}{4}}(12,-1)\equiv\begin{cases}\mp 2\cdot 37^{\frac{p-1}{8}}\frac{d}{c}\pmod p & \text{if } 2\mid y \text{ and } \frac{d-6c}{x}\equiv\pm 1,\pm 7,\pm 9,\pm 10,\\ & \quad\pm 12,\pm 16,\pm 26,\pm 33,\pm 34\pmod{37},\\ \pm 2\cdot 37^{\frac{p-1}{8}}\pmod p & \text{if } 2\mid y \text{ and } \frac{d-6c}{x}\equiv\pm 2,\pm 14,\pm 15,\pm 18,\\ & \quad\pm 20,\pm 24,\pm 29,\pm 31,\pm 32\pmod{37},\\ 0\pmod p & \text{if } 2\nmid y.\end{cases}$$

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

$$U_{\frac{p-1}{4}}(12,-1) \equiv \begin{cases} \pm 37^{\frac{p-5}{8}}\frac{d}{c} \pmod p & \textit{if } 2 \mid y \textit{ and } \frac{d-6c}{x} \equiv \pm 1, \pm 7, \pm 9, \pm 10, \\ & \quad \pm 12, \pm 16, \pm 26, \pm 33, \pm 34 \pmod{37}, \\ \mp 37^{\frac{p-5}{8}} \pmod p & \textit{if } 2 \mid y \textit{ and } \frac{d-6c}{x} \equiv \pm 2, \pm 14, \pm 15, \pm 18, \\ & \quad \pm 20, \pm 24, \pm 29, \pm 31, \pm 32 \pmod{37}, \\ 0 \pmod p & \textit{if } 2 \nmid y \end{cases}$$

and

$$V_{\frac{p-1}{4}}(12,-1) \equiv \begin{cases} \pm 2\cdot 37^{\frac{p-5}{8}}\frac{dx}{cy} \pmod p & \textit{if } 2 \nmid y \textit{ and } \frac{d-6c}{x} \equiv \pm 1, \pm 7, \pm 9, \pm 10, \\ & \quad \pm 12, \pm 16, \pm 26, \pm 33, \pm 34 \pmod{37}, \\ \mp 2\cdot 37^{\frac{p-5}{8}}\frac{x}{y} \pmod p & \textit{if } 2 \nmid y \textit{ and } \frac{d-6c}{x} \equiv \pm 2, \pm 14, \pm 15, \pm 18, \\ & \quad \pm 20, \pm 24, \pm 29, \pm 31, \pm 32 \pmod{37}, \\ 0 \pmod p & \textit{if } 2 \mid y. \end{cases}$$

Proof. Observe that for $A \in \mathbb{Z}$,

$$\left(\frac{A}{1-6i}\right)_4 = \begin{cases} \pm 1 & \text{if } A \equiv \pm 1, \pm 7, \pm 9, \pm 10, \\ & \pm 12, \pm 16, \pm 26, \pm 33, \pm 34 \pmod{37}, \\ \pm i & \text{if } A \equiv \pm 2, \pm 14, \pm 15, \pm 18, \\ & \pm 20, \pm 24, \pm 29, \pm 31, \pm 32 \pmod{37}. \end{cases} \tag{7.5}$$

Taking $a = 3$ in Theorem 7.3 we obtain the result. □

Theorem 7.4. *Let $a \in \mathbb{Z}$. 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 $4a^2 + 1 \neq p$. Suppose $x = 2^{\alpha}x_0$ and $x_0 \equiv 1 \pmod 4$.*

(i) *If $2 \mid a$, then*

$$\begin{aligned} p \mid U_{\frac{p-1}{8}}(4a,-1) &\iff \left(2a+\sqrt{4a^2+1}\right)^{\frac{p-1}{4}} \equiv (-1)^{\frac{p-1}{8}} \pmod p \\ &\iff \left(-1-4a^2\right)^{\frac{p-1}{8}} \equiv \begin{cases} \pm(-1)^{\frac{a}{2}(x-1)} \pmod p & \textit{if } \left(\frac{(d-2ac)/x}{1-2ai}\right)_4 = \pm 1, \\ \pm(-1)^{\frac{a}{2}(x-1)}\frac{c}{d} \pmod p & \textit{if } \left(\frac{(d-2ac)/x}{1-2ai}\right)_4 = \pm i. \end{cases} \end{aligned}$$

(ii) *If $2 \nmid a$, then*

$$\begin{aligned} p \mid U_{\frac{p-1}{8}}(4a,-1) &\iff \left(2a+\sqrt{4a^2+1}\right)^{\frac{p-1}{4}} \equiv (-1)^{\frac{p-1}{8}} \pmod p \\ &\iff 2 \nmid x \textit{ and } \left(-1-4a^2\right)^{\frac{p-1}{8}} \equiv \begin{cases} \pm 1 \pmod p & \textit{if } \left(\frac{(d-2ac)/x}{1-2ai}\right)_4 = \pm i, \\ \pm\frac{d}{c} \pmod p & \textit{if } \left(\frac{(d-2ac)/x}{1-2ai}\right)_4 = \pm 1. \end{cases} \end{aligned}$$

Proof. As $(2a+\sqrt{4a^2+1})(2a-\sqrt{4a^2+1}) = -1$, from (1.3) we see that

$$\begin{aligned} p \mid U_{\frac{p-1}{8}}(4a,-1) &\iff \left(2a+\sqrt{4a^2+1}\right)^{\frac{p-1}{8}} \equiv \left(2a-\sqrt{4a^2+1}\right)^{\frac{p-1}{8}} \pmod p \\ &\iff \left(2a+\sqrt{4a^2+1}\right)^{\frac{p-1}{4}} \equiv (-1)^{\frac{p-1}{8}} \pmod p. \end{aligned}$$

By (1.5) we have

$$p \mid U_{\frac{p-1}{8}}(4a,-1) \iff V_{\frac{p-1}{4}}(4a,-1) \equiv 2(-1)^{\frac{p-1}{8}} \pmod p.$$

Now putting the above together with Theorem 7.3(i) and the fact $(-1)^y = (-1)^{x-1}$ we deduce the result. □

Putting $a=3$ in Theorem 7.4 and then applying (7.5) we deduce the following result.

Corollary 7.2. *Let p be a prime such that $p \equiv 1, 9, 25, 33, 41, 49, 65, 73, 81, 121, 137, 145, 169, 201, 225, 233, 249, 289 \pmod{296}$ and hence $p = c^2 + d^2 = x^2 + 37y^2$ for some $c, d, x, y \in \mathbb{Z}$. Suppose $c \equiv 1 \pmod 4$, $x = 2^{\alpha} x_0$, $y = 2^{\beta} y_0$ and $x_0 \equiv y_0 \equiv 1 \pmod 4$. Then*

$$\begin{aligned} & p \mid U_{\frac{p-1}{8}}(12,-1) \\ & \iff \left(6+\sqrt{37}\right)^{\frac{p-1}{4}} \equiv (-1)^{\frac{p-1}{8}} \pmod p \\ & \iff 2 \nmid x \text{ and } (-37)^{\frac{p-1}{8}} \equiv \begin{cases} \pm\frac{d}{c} \pmod p & \text{if } \frac{d-6c}{x} \equiv \pm 1, \pm 7, \pm 9, \pm 10, \pm 12, \\ & \qquad \pm 16, \pm 26, \pm 33, \pm 34 \pmod{37}, \\ \pm 1 \pmod p & \text{if } \frac{d-6c}{x} \equiv \pm 2, \pm 14, \pm 15, \pm 18, \pm 20, \\ & \qquad \pm 24, \pm 29, \pm 31, \pm 32 \pmod{37}. \end{cases} \end{aligned}$$

Corollary 7.3. *Let $p \equiv 1 \pmod 8$ be a prime such that $p = c^2 + d^2 = x^2 + 17y^2$ with $c, d, x, y \in \mathbb{Z}$, $c \equiv 1 \pmod 4$ and $p \neq 17$. Suppose $x = 2^{\alpha} x_0$ and $x_0 \equiv 1 \pmod 4$. Then*

$$\begin{aligned} & p \mid U_{\frac{p-1}{8}}(8,-1) \\ & \iff (4+\sqrt{17})^{\frac{p-1}{4}} \equiv (-1)^{\frac{p-1}{8}} \pmod p \\ & \iff (-17)^{\frac{p-1}{8}} \equiv \begin{cases} (-1)^x \pmod p & \text{if } \frac{d-4c}{x} \equiv \pm 2, \pm 8 \pmod{17}, \\ -(-1)^x \pmod p & \text{if } \frac{d-4c}{x} \equiv \pm 1, \pm 4 \pmod{17}, \\ (-1)^x \frac{c}{d} \pmod p & \text{if } \frac{d-4c}{x} \equiv \pm 6, \pm 7 \pmod{17}, \\ -(-1)^x \frac{c}{d} \pmod p & \text{if } \frac{d-4c}{x} \equiv \pm 3, \pm 5 \pmod{17}. \end{cases} \end{aligned}$$

Proof. Observe that for $A \in \mathbb{Z}$,

$$\left(\frac{A}{1-4i}\right)_4 = \begin{cases} 1 & \text{if } A \equiv \pm 1, \pm 4 \pmod{17}, \\ -1 & \text{if } A \equiv \pm 2, \pm 8 \pmod{17}, \\ i & \text{if } A \equiv \pm 3, \pm 5 \pmod{17}, \\ -i & \text{if } A \equiv \pm 6, \pm 7 \pmod{17}. \end{cases} \tag{7.6}$$

Taking $a=2$ in Theorem 7.4 we obtain the result. □

8. Congruences for $U_{\frac{p-1}{4}}(2a,-k^2)$ and $V_{\frac{p-1}{4}}(2a,-k^2)$ (mod p) when $2\nmid ak$

Theorem 8.1. *Let $p\equiv 1 \pmod 8$ be a prime, and $p=c^2+d^2$ with $c,d\in\mathbb{Z}$ and $c\equiv 1 \pmod 4$. Let $a,k\in\mathbb{Z}$, $2\nmid ak$, $(a,k)=1$, $4\mid a+k$ and $p\nmid k$. Assume $p=x^2+(a^2+k^2)y^2$ with $x,y\in\mathbb{Z}$, $x\equiv 1 \pmod 4$, $y=2^{\beta}y_0$ and $y_0\equiv 1 \pmod 4$. Suppose $(\frac{x+ayi}{k})_4(\frac{(\frac{k-a}{2}d-\frac{k+a}{2}c)/x}{\frac{k-a}{2}+\frac{k+a}{2}i})_4=i^m$. Then*

$$\left(a-\frac{cx}{dy}\right)^{\frac{p-1}{4}}\equiv\begin{cases}(-1)^{\frac{a+1}{2}+\frac{a-1}{2}\cdot\frac{a+k}{4}}k^{\frac{p-1}{4}}\left(-\frac{a^2+k^2}{2}\right)^{\frac{p-1}{8}}(c/d)^{(1-(-1)^{\frac{a+k}{4}})/2-1+m} \pmod p & \text{if } 2\parallel y,\\ (-1)^{\frac{a-1}{2}\cdot\frac{a+k}{4}+\frac{y}{4}}k^{\frac{p-1}{4}}\left(-\frac{a^2+k^2}{2}\right)^{\frac{p-1}{8}}(c/d)^{(1-(-1)^{\frac{a+k}{4}})/2+m} \pmod p & \text{if } 4\mid y.\end{cases}$$

Proof. Suppose $(\frac{\frac{k-a}{2}d-\frac{k+a}{2}c}{\frac{k-a}{2}+\frac{k+a}{2}i})_4=i^s$. According to Theorem 4.2 and the fact $4\mid d$ we have

$$\begin{aligned}(-a-kc/d)^{-\frac{p-1}{4}}&\equiv(-1)^{\frac{k-1}{2}\cdot\frac{d}{2}+\frac{a-1}{2}\cdot\frac{a+k}{4}}(c/d)^{((-1)^{\frac{d}{2}}(c-d)-1-d^2)/4+(1-(-1)^{\frac{a+k}{4}})/2+s}\\&\equiv(-1)^{\frac{a-1}{2}\cdot\frac{a+k}{4}}(c/d)^{(c-d-1)/4+(1-(-1)^{\frac{a+k}{4}})/2+s} \pmod p.\end{aligned}$$

As $p=c^2+16(d/4)^2$ we see that

$$(-1)^{\frac{p-1}{8}}=(-1)^{\frac{c^2-1}{8}}=(-1)^{\frac{c-1}{4}\cdot\frac{c+1}{2}}=(-1)^{\frac{c-1}{4}}$$

and

$$\begin{aligned}(c/d)^{\frac{p-1}{8}-\frac{c-1}{4}}&=(c/d)^{\frac{c^2-1+d^2}{8}-\frac{c-1}{4}}=(c/d)^{\frac{c-1}{4}\cdot\frac{c-1}{2}+2(d/4)^2}\\&\equiv(-1)^{(\frac{d}{4})^2+(\frac{c-1}{4})^2}=(-1)^{\frac{d}{4}+\frac{c-1}{4}}=(-1)^{\frac{d}{4}+\frac{p-1}{8}} \pmod p.\end{aligned}$$

Thus

$$(c/d)^{\frac{c-d-1}{4}}\equiv(-1)^{\frac{d}{4}+\frac{p-1}{8}}(c/d)^{\frac{p-1}{8}}\cdot(c/d)^{-\frac{d}{4}}\equiv(c/d)^{\frac{d}{4}-\frac{p-1}{8}} \pmod p.$$

Hence

$$\left(-a-k\frac{c}{d}\right)^{-\frac{p-1}{4}}\equiv(-1)^{\frac{a-1}{2}\cdot\frac{a+k}{4}}(c/d)^{\frac{d}{4}-\frac{p-1}{8}+(1-(-1)^{\frac{a+k}{4}})/2+s} \pmod p. \tag{8.1}$$

As $(c/d)^2\equiv -1 \pmod p$ and $(x/y)^2\equiv -a^2-k^2 \pmod p$, it is easily seen that

$$\left(-a-k\frac{c}{d}\right)\frac{a-cx/(dy)}{2}\equiv\left(\frac{x/y-k+ac/d}{2}\right)^2 \pmod p.$$

Thus

$$\left(a-\frac{cx}{dy}\right)^{\frac{p-1}{4}}\equiv\left(-a-k\frac{c}{d}\right)^{-\frac{p-1}{4}}\cdot 2^{-\frac{p-1}{4}}\left(\frac{x}{y}-k+a\frac{c}{d}\right)^{\frac{p-1}{2}} \pmod p. \tag{8.2}$$

By Theorem 5.1(iii) and the fact $(\frac{x}{\frac{a-k}{2}+\frac{a+k}{2}i})_4=(\frac{x}{\frac{k-a}{2}+\frac{k+a}{2}i})_4^{-1}$ we have

$$\left(\frac{x/y-k+ai}{p}\right)_4=\left(\frac{x-ky+ayi}{p}\right)_4$$
$$=\begin{cases}(-1)^{\frac{k+1}{2}}i^{\frac{x-1}{4}}\big(\frac{x+ayi}{k}\big)_4\big(\frac{x}{\frac{a-k}{2}+\frac{a+k}{2}i}\big)_4 & \text{if } 2\parallel y,\\ (-1)^{\frac{y}{4}}i^{\frac{x-1}{4}}\big(\frac{x+ayi}{k}\big)_4\big(\frac{x}{\frac{a-k}{2}+\frac{a+k}{2}i}\big)_4 & \text{if } 4\mid y\end{cases}$$
$$=\begin{cases}(-1)^{\frac{k+1}{2}}i^{\frac{x-1}{4}+m-s} & \text{if } 2\parallel y,\\ (-1)^{\frac{y}{4}}i^{\frac{x-1}{4}+m-s} & \text{if } 4\mid y.\end{cases}$$

Applying Lemma 6.1 we see that

$$(x/y-k+ac/d)^{\frac{p-1}{2}}$$
$$\equiv\begin{cases}(-1)^{\frac{k+1}{2}}(2k)^{\frac{p-1}{4}}(-a^2-k^2)^{\frac{p-1}{8}}(c/d)^{\frac{x-1}{4}+m-s}\pmod p & \text{if } 2\parallel y,\\ (-1)^{\frac{y}{4}}(2k)^{\frac{p-1}{4}}(-a^2-k^2)^{\frac{p-1}{8}}(c/d)^{\frac{x-1}{4}+m-s}\pmod p & \text{if } 4\mid y.\end{cases}$$

As

$$(c/d)^{\frac{p-1}{8}-\frac{x-1}{4}}=(c/d)^{\frac{x^2-1+(a^2+k^2)y^2}{8}-\frac{x-1}{4}}\equiv(c/d)^{\frac{x^2-1}{8}-\frac{x-1}{4}+\frac{y^2}{4}}$$
$$\equiv(-1)^{\frac{x-1}{4}}(c/d)^{\frac{y^2}{4}}\pmod p$$

and

$$(-1)^{\frac{x-1}{4}}=(-1)^{\frac{x^2-1}{8}}=(-1)^{\frac{p-1-(a^2+k^2)y^2}{8}}=(-1)^{\frac{p-1}{8}-\frac{y^2}{4}}=(-1)^{\frac{p-1}{8}-\frac{y}{2}},$$

we see that

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

Since Gauss it is known that (see [L1] and [HW3, (1.4) and (1.5)])

$$2^{\frac{p-1}{8}}\equiv(-1)^{\frac{p-1}{8}}(c/d)^{-\frac{d}{4}}\pmod p.$$

Thus

$$\left(-a^2-k^2\right)^{\frac{p-1}{8}}=(-2)^{\frac{p-1}{8}}\left(\frac{a^2+k^2}{2}\right)^{\frac{p-1}{8}}\equiv(c/d)^{-\frac{d}{4}}\left(\frac{a^2+k^2}{2}\right)^{\frac{p-1}{8}}\pmod p.$$

Hence, by the above we obtain

$$2^{-\frac{p-1}{4}}(x/y-k+ac/d)^{\frac{p-1}{2}}\equiv\begin{cases}(-1)^{\frac{k-1}{2}}k^{\frac{p-1}{4}}(-\frac{a^2+k^2}{2})^{\frac{p-1}{8}}(c/d)^{-\frac{d}{4}+\frac{p-1}{8}-1+m-s}\pmod p & \text{if } 2\parallel y,\\ (-1)^{\frac{y}{4}}k^{\frac{p-1}{4}}(-\frac{a^2+k^2}{2})^{\frac{p-1}{8}}(c/d)^{-\frac{d}{4}+\frac{p-1}{8}+m-s}\pmod p & \text{if } 4\mid y.\end{cases}$$

This together with (8.1) and (8.2) yields the result. □

Theorem 8.2. *Let $p \equiv 1 \pmod 8$ be a prime, and $p = c^2 + d^2$ with $c, d \in \mathbb{Z}$ and $c \equiv 1 \pmod 4$. Let $a, k \in \mathbb{Z}$, $2 \nmid ak$, $(a,k) = 1$, $4 \mid a + k$ and $p \nmid k$. Assume $p = x^2 + (a^2 + k^2)y^2$ with $x, y \in \mathbb{Z}$, $x \equiv 1 \pmod 4$, $y = 2^\beta y_0$ and $y_0 \equiv 1 \pmod 4$. Suppose $(\frac{x+ayi}{k})_4(\frac{(\frac{k-a}{2}d - \frac{k+a}{2}c)/x}{\frac{k-a}{2} + \frac{k+a}{2}i})_4 = i^m$. Then*

$$U_{\frac{p-1}{4}}\big(2a, -k^2\big) \equiv \begin{cases} \frac{1+(\frac{k}{p})}{2}(-1)^{\frac{a+1}{2} + \frac{a-1}{2}\cdot\frac{a+k}{4}} k^{\frac{p-1}{4}} \big(-\frac{a^2+k^2}{2}\big)^{\frac{p-1}{8}} (c/d)^{m+(1-(-1)^{\frac{a+k}{4}})/2} \frac{y}{x} \pmod p & \text{if } 2 \parallel y, \\ \frac{(\frac{k}{p})-1}{2}(-1)^{\frac{a-1}{2}\cdot\frac{a+k}{4} + \frac{y}{4}} k^{\frac{p-1}{4}} \big(-\frac{a^2+k^2}{2}\big)^{\frac{p-1}{8}} (c/d)^{m-1+(1-(-1)^{\frac{a+k}{4}})/2} \frac{y}{x} \pmod p & \text{if } 4 \mid y \end{cases}$$

and

$$V_{\frac{p-1}{4}}\big(2a, -k^2\big) \equiv \begin{cases} (1 - (\frac{k}{p}))(-1)^{\frac{a+1}{2} + \frac{a-1}{2}\cdot\frac{a+k}{4}} k^{\frac{p-1}{4}} \big(-\frac{a^2+k^2}{2}\big)^{\frac{p-1}{8}} (c/d)^{m-1+(1-(-1)^{\frac{a+k}{4}})/2} \pmod p & \text{if } 2 \parallel y, \\ (1 + (\frac{k}{p}))(-1)^{\frac{a-1}{2}\cdot\frac{a+k}{4} + \frac{y}{4}} k^{\frac{p-1}{4}} \big(-\frac{a^2+k^2}{2}\big)^{\frac{p-1}{8}} (c/d)^{m+(1-(-1)^{\frac{a+k}{4}})/2} \pmod p & \text{if } 4 \mid y. \end{cases}$$

Proof. As

$$\begin{aligned} &\left(\frac{x+ayi}{k}\right)_4 \left(\frac{(\frac{k-a}{2}(-d) - \frac{k+a}{2}c)/x}{\frac{k-a}{2} + \frac{k+a}{2}i}\right)_4 \cdot \left(\frac{x+ayi}{k}\right)_4 \left(\frac{(\frac{k-a}{2}d - \frac{k+a}{2}c)/x}{\frac{k-a}{2} + \frac{k+a}{2}i}\right)_4 \\ &= \left(\frac{x+ayi}{k}\right)_4^2 \left(\frac{(\frac{k+a}{2})^2c^2 - (\frac{k-a}{2})^2d^2}{\frac{k-a}{2} + \frac{k+a}{2}i}\right)_4 \left(\frac{x^2}{\frac{k-a}{2} + \frac{k+a}{2}i}\right)_4^{-1} \\ &= \left(\frac{x^2 + a^2y^2}{k}\right) \left(\frac{-(\frac{k-a}{2})^2 p}{\frac{k-a}{2} + \frac{k+a}{2}i}\right)_4 \left(\frac{x^2}{\frac{k-a}{2} + \frac{k+a}{2}i}\right)_4^{-1} \\ &= \left(\frac{p - k^2y^2}{k}\right)(-1)^{\frac{k+a}{4}} \left(\frac{\frac{k-a}{2} + \frac{k+a}{2}i}{\frac{k-a}{2}}\right)_4^2 \left(\frac{x^2 + (k^2+a^2)y^2}{\frac{k-a}{2} + \frac{k+a}{2}i}\right)_4 \left(\frac{x^2}{\frac{k-a}{2} + \frac{k+a}{2}i}\right)_4^{-1} \\ &= (-1)^{\frac{k+a}{4}} \left(\frac{p}{k}\right), \end{aligned}$$

we have

$$\left(\frac{x+ayi}{k}\right)_4 \left(\frac{(\frac{k-a}{2}(-d) - \frac{k+a}{2}c)/x}{\frac{k-a}{2} + \frac{k+a}{2}i}\right)_4 = (-1)^{\frac{k+a}{4}} \left(\frac{k}{p}\right) i^{-m} = i^{m'},$$

where $m' = \frac{k+a}{2} + 1 - (\frac{k}{p}) - m$. Setting $d' = -d$ we then have

$$\begin{aligned} &(c/d')^{(1-(-1)^{\frac{a+k}{4}})/2+m'} \\ &= (-c/d)^{(1-(-1)^{\frac{a+k}{4}})/2 + \frac{a+k}{2} + 1 - (\frac{k}{p}) - m} \\ &= (-1)^{(1-(-1)^{\frac{a+k}{4}})/2} (c/d)^{(1-(-1)^{\frac{a+k}{4}})/2} \cdot (-1)^{\frac{a+k}{4}} \left(\frac{k}{p}\right)(-c/d)^{-m} \\ &\equiv \left(\frac{k}{p}\right)(c/d)^{(1-(-1)^{\frac{a+k}{4}})/2+m} \pmod p. \end{aligned}$$

Thus, by Theorem 8.1 we obtain

$$\left(a+\frac{cx}{dy}\right)^{\frac{p-1}{4}} \equiv \begin{cases} -(\frac{k}{p})(-1)^{\frac{a+1}{2}+\frac{a-1}{2}\cdot\frac{a+k}{4}}k^{\frac{p-1}{4}}\big(-\frac{a^2+k^2}{2}\big)^{\frac{p-1}{8}}(c/d)^{(1-(-1)^{\frac{a+k}{4}})/2-1+m} \pmod p \\ \quad \text{if } 2 \parallel y, \\ (\frac{k}{p})(-1)^{\frac{a-1}{2}\cdot\frac{a+k}{4}+\frac{y}{4}}k^{\frac{p-1}{4}}\big(-\frac{a^2+k^2}{2}\big)^{\frac{p-1}{8}}(c/d)^{(1-(-1)^{\frac{a+k}{4}})/2+m} \pmod p \\ \quad \text{if } 4 \mid y. \end{cases} \tag{8.3}$$

From (1.3) and (1.4) we know that

$$\begin{aligned} U_{\frac{p-1}{4}}(2a,-k^2) &= \frac{1}{2\sqrt{a^2+k^2}}\big\{\big(a+\sqrt{a^2+k^2}\big)^{\frac{p-1}{4}}-\big(a-\sqrt{a^2+k^2}\big)^{\frac{p-1}{4}}\big\} \\ &\equiv \frac{dy}{2cx}\left\{\left(a+\frac{cx}{dy}\right)^{\frac{p-1}{4}}-\left(a-\frac{cx}{dy}\right)^{\frac{p-1}{4}}\right\} \pmod p \end{aligned}$$

and

$$\begin{aligned} V_{\frac{p-1}{4}}\big(2a,-k^2\big) &= \big(a+\sqrt{a^2+k^2}\big)^{\frac{p-1}{4}}+\big(a-\sqrt{a^2+k^2}\big)^{\frac{p-1}{4}} \\ &\equiv \left(a+\frac{cx}{dy}\right)^{\frac{p-1}{4}}+\left(a-\frac{cx}{dy}\right)^{\frac{p-1}{4}} \pmod p. \end{aligned}$$

This together with Theorem 8.1 and (8.3) gives the result. □

Putting $k=(-1)^{\frac{a+1}{2}}$ in Theorem 8.2 and noting that $(\frac{(\frac{1-a}{2}d-\frac{1+a}{2}c)/x}{\frac{1-a}{2}+\frac{1+a}{2}i})_4=(-1)^{\frac{a+1}{4}}(\frac{(\frac{a+1}{2}c+\frac{a-1}{2}d)/x}{\frac{a-1}{2}-\frac{a+1}{2}i})_4$ for $a\equiv 3 \pmod 4$ we deduce the following result.

Theorem 8.3. *Let $p\equiv 1 \pmod 8$ be a prime, and $p=c^2+d^2$ with $c,d\in\mathbb{Z}$ and $c\equiv 1 \pmod 4$. Let $a\in\mathbb{Z}$ with $2\nmid a$. Assume $p=x^2+(a^2+1)y^2$ with $x,y\in\mathbb{Z}$, $x\equiv 1 \pmod 4$, $y=2^\beta y_0$ and $y_0\equiv 1 \pmod 4$.*

(i) *If $a\equiv 1 \pmod 4$, then*

$$U_{\frac{p-1}{4}}(2a,-1) \equiv \begin{cases} \mp\big(-\frac{a^2+1}{2}\big)^{\frac{p-1}{8}}(c/d)^{(1-(-1)^{\frac{a-1}{4}})/2}\frac{y}{x} \pmod p \\ \quad \textit{if } 2 \parallel y \textit{ and } \big(\frac{(\frac{1-a}{2}c-\frac{1+a}{2}d)/x}{\frac{1+a}{2}+\frac{1-a}{2}i}\big)_4=\pm 1, \\ \mp\big(-\frac{a^2+1}{2}\big)^{\frac{p-1}{8}}(c/d)^{1+(1-(-1)^{\frac{a-1}{4}})/2}\frac{y}{x} \pmod p \\ \quad \textit{if } 2 \parallel y \textit{ and } \big(\frac{(\frac{1-a}{2}c-\frac{1+a}{2}d)/x}{\frac{1+a}{2}+\frac{1-a}{2}i}\big)_4=\pm i, \\ 0 \pmod p \quad \textit{if } 4 \mid y \end{cases}$$

and

$$V_{\frac{p-1}{4}}(2a,-1) \equiv \begin{cases} 0 \pmod p \quad \textit{if } 2 \parallel y \\ \pm 2(-1)^{\frac{y}{4}}\big(-\frac{a^2+1}{2}\big)^{\frac{p-1}{8}}(c/d)^{(1-(-1)^{\frac{a-1}{4}})/2} \pmod p \\ \quad \textit{if } 4 \mid y \textit{ and } \big(\frac{(\frac{1-a}{2}c-\frac{1+a}{2}d)/x}{\frac{1+a}{2}+\frac{1-a}{2}i}\big)_4=\pm 1, \\ \pm 2(-1)^{\frac{y}{4}}\big(-\frac{a^2+1}{2}\big)^{\frac{p-1}{8}}(c/d)^{1+(1-(-1)^{\frac{a-1}{4}})/2} \pmod p \\ \quad \textit{if } 4 \mid y \textit{ and } \big(\frac{(\frac{1-a}{2}c-\frac{1+a}{2}d)/x}{\frac{1+a}{2}+\frac{1-a}{2}i}\big)_4=\pm i. \end{cases}$$

(ii) *If* $a \equiv 3 \pmod 4$, *then*

$$U_{\frac{p-1}{4}}(2a,-1) \equiv \begin{cases} \pm\bigl(-\frac{a^2+1}{2}\bigr)^{\frac{p-1}{8}}(c/d)^{(1-(-1)^{\frac{a+1}{4}})/2}\frac{y}{x} \pmod p \\ \quad \textit{if}\ 2 \parallel y\ \textit{and}\ \Bigl(\frac{(\frac{a+1}{2}c+\frac{a-1}{2}d)/x}{\frac{a-1}{2}-\frac{a+1}{2}i}\Bigr)_4 = \pm 1, \\ \pm\bigl(-\frac{a^2+1}{2}\bigr)^{\frac{p-1}{8}}(c/d)^{1+(1-(-1)^{\frac{a+1}{4}})/2}\frac{y}{x} \pmod p \\ \quad \textit{if}\ 2 \parallel y\ \textit{and}\ \Bigl(\frac{(\frac{a+1}{2}c+\frac{a-1}{2}d)/x}{\frac{a-1}{2}-\frac{a+1}{2}i}\Bigr)_4 = \pm i, \\ 0 \pmod p \quad \textit{if}\ 4 \mid y \end{cases}$$

and

$$V_{\frac{p-1}{4}}(2a,-1) \equiv \begin{cases} 0 \pmod p \quad \textit{if}\ 2 \parallel y \\ \pm 2(-1)^{\frac{y}{4}}\bigl(-\frac{a^2+1}{2}\bigr)^{\frac{p-1}{8}}(c/d)^{(1-(-1)^{\frac{a+1}{4}})/2} \pmod p \\ \quad \textit{if}\ 4 \mid y\ \textit{and}\ \Bigl(\frac{(\frac{a+1}{2}c+\frac{a-1}{2}d)/x}{\frac{a-1}{2}-\frac{a+1}{2}i}\Bigr)_4 = \pm 1, \\ \pm 2(-1)^{\frac{y}{4}}\bigl(-\frac{a^2+1}{2}\bigr)^{\frac{p-1}{8}}(c/d)^{1+(1-(-1)^{\frac{a+1}{4}})/2} \pmod p \\ \quad \textit{if}\ 4 \mid y\ \textit{and}\ \Bigl(\frac{(\frac{a+1}{2}c+\frac{a-1}{2}d)/x}{\frac{a-1}{2}-\frac{a+1}{2}i}\Bigr)_4 = \pm i. \end{cases}$$

Corollary 8.1. *Let* $p \equiv 1, 9 \pmod{40}$ *be a prime and hence* $p = c^2 + d^2 = x^2 + 10y^2$ *with* $c, d, x, y \in \mathbb{Z}$. *Suppose* $c \equiv x \equiv 1 \pmod 4$, $y = 2^\beta y_0$ *and* $y_0 \equiv 1 \pmod 4$. *Then*

$$U_{\frac{p-1}{4}}(6,-1) \equiv \begin{cases} \pm(-5)^{\frac{p-1}{8}}\frac{cy}{dx} \pmod p & \textit{if}\ 2 \parallel y\ \textit{and}\ x \equiv \pm d \pmod 5, \\ \pm(-5)^{\frac{p-1}{8}}\frac{y}{x} \pmod p & \textit{if}\ 2 \parallel y\ \textit{and}\ x \equiv \pm c \pmod 5, \\ 0 \pmod p & \textit{if}\ 4 \mid y \end{cases}$$

and

$$V_{\frac{p-1}{4}}(6,-1) \equiv \begin{cases} 0 \pmod p & \textit{if}\ 2 \parallel y, \\ \pm 2(-1)^{\frac{y}{4}}(-5)^{\frac{p-1}{8}}\frac{c}{d} \pmod p & \textit{if}\ 4 \mid y\ \textit{and}\ x \equiv \pm d \pmod 5, \\ \pm 2(-1)^{\frac{y}{4}}(-5)^{\frac{p-1}{8}} \pmod p & \textit{if}\ 4 \mid y\ \textit{and}\ x \equiv \pm c \pmod 5. \end{cases}$$

Proof. As $p \equiv 1, 9 \pmod{40}$, we see that $5 \mid cd$. Clearly $5 \mid c$ if and only if $x \equiv \pm d \pmod 5$, and $5 \mid d$ if and only if $x \equiv \pm c \pmod 5$. Thus

$$\left(\frac{(2c+d)/x}{1-2i}\right)_4 = \begin{cases} \bigl(\frac{\pm 1}{1-2i}\bigr)_4 = \pm 1 & \text{if } x \equiv \pm d \pmod 5, \\ \bigl(\frac{\pm 2}{1-2i}\bigr)_4 = \mp i & \text{if } x \equiv \pm c \pmod 5. \end{cases} \tag{8.4}$$

Now putting $a = 3$ in Theorem 8.3(ii) and applying the above we deduce the result. □

Theorem 8.4. *Let $p \equiv 1 \pmod 8$ be a prime, and $p = c^2 + d^2$ with $c, d \in \mathbb{Z}$ and $c \equiv 1 \pmod 4$. Let $a \in \mathbb{Z}$ with $2 \nmid a$. Assume $p = x^2 + (a^2+1)y^2$ with $x, y \in \mathbb{Z}$ and $x \equiv 1 \pmod 4$.*

(i) *If $a \equiv 1 \pmod 4$, then*

$$\begin{aligned}
&p \mid U_{\frac{p-1}{8}}(2a, -1) \\
&\iff \left(a + \sqrt{a^2+1}\right)^{\frac{p-1}{4}} \equiv (-1)^{\frac{p-1}{8}} \pmod p \\
&\iff 4 \mid y \text{ and } \left(\frac{a^2+1}{2}\right)^{\frac{p-1}{8}} \equiv \begin{cases} \pm(-1)^{\frac{y}{4}}(d/c)^{(1-(-1)^{\frac{a-1}{4}})/2} \pmod p \\ \quad \textit{if } \left(\frac{(\frac{1-a}{2}c - \frac{1+a}{2}d)/x}{\frac{1+a}{2} + \frac{1-a}{2}i}\right)_4 = \pm 1, \\ \pm(-1)^{\frac{y}{4}}(d/c)^{1+(1-(-1)^{\frac{a-1}{4}})/2} \pmod p \\ \quad \textit{if } \left(\frac{(\frac{1-a}{2}c - \frac{1+a}{2}d)/x}{\frac{1+a}{2} + \frac{1-a}{2}i}\right)_4 = \pm i. \end{cases}
\end{aligned}$$

(ii) *If $a \equiv 3 \pmod 4$, then*

$$\begin{aligned}
&p \mid U_{\frac{p-1}{8}}(2a, -1) \\
&\iff \left(a + \sqrt{a^2+1}\right)^{\frac{p-1}{4}} \equiv (-1)^{\frac{p-1}{8}} \pmod p \\
&\iff 4 \mid y \text{ and } \left(\frac{a^2+1}{2}\right)^{\frac{p-1}{8}} \equiv \begin{cases} \pm(-1)^{\frac{y}{4}}(d/c)^{(1-(-1)^{\frac{a+1}{4}})/2} \pmod p \\ \quad \textit{if } \left(\frac{(\frac{a+1}{2}c + \frac{a-1}{2}d)/x}{\frac{a-1}{2} - \frac{a+1}{2}i}\right)_4 = \pm 1, \\ \pm(-1)^{\frac{y}{4}}(d/c)^{1+(1-(-1)^{\frac{a+1}{4}})/2} \pmod p \\ \quad \textit{if } \left(\frac{(\frac{a+1}{2}c + \frac{a-1}{2}d)/x}{\frac{a-1}{2} - \frac{a+1}{2}i}\right)_4 = \pm i. \end{cases}
\end{aligned}$$

Proof. From (1.3) we see that

$$\begin{aligned}
p \mid U_{\frac{p-1}{8}}(2a, -1) &\iff \left(a + \sqrt{a^2+1}\right)^{\frac{p-1}{8}} \equiv \left(a - \sqrt{a^2+1}\right)^{\frac{p-1}{8}} \pmod p \\
&\iff \left(a + \sqrt{a^2+1}\right)^{\frac{p-1}{4}} \equiv (-1)^{\frac{p-1}{8}} \pmod p.
\end{aligned}$$

By (1.5) we have

$$p \mid U_{\frac{p-1}{8}}(2a, -1) \iff V_{\frac{p-1}{4}}(2a, -1) \equiv 2(-1)^{\frac{p-1}{8}} \pmod p.$$

Now applying Theorem 8.3 and the above we deduce the result. □

Putting $a = 3$ in Theorem 8.4 and then applying (8.4) we have:

Corollary 8.2. *Let $p \equiv 1, 9 \pmod{40}$ be a prime and hence $p = c^2 + d^2 = x^2 + 10y^2$ for $c, d, x, y \in \mathbb{Z}$. Suppose $c \equiv x \equiv 1 \pmod 4$. Then $p \mid U_{\frac{p-1}{8}}(6, -1)$ if and only if $4 \mid y$ and*

$$5^{\frac{p-1}{8}} \equiv \begin{cases} \pm(-1)^{\frac{y}{4}} \frac{d}{c} \pmod p & \textit{if } x \equiv \pm d \pmod 5, \\ \pm(-1)^{\frac{y}{4}} \pmod p & \textit{if } x \equiv \pm c \pmod 5. \end{cases}$$

Theorem 8.5. *Let $p \equiv 1, 9 \pmod{40}$ be a prime and hence $p = C^2 + 2D^2 = x^2 + 10y^2$ with $C, D, x, y \in \mathbb{Z}$. Suppose $C \equiv x \equiv 1 \pmod 4$, $y = 2^\beta y_0$ and $y_0 \equiv 1 \pmod 4$. Then*

$$U_{\frac{p-1}{4}}(6, -1) \equiv \begin{cases} \mp(-1)^{\frac{C-1}{4}}(\frac{x}{5})\frac{y}{x} \pmod p & \text{if } 2 \parallel y \text{ and } x \equiv \pm C, \pm 3C \pmod 5, \\ 0 \pmod p & \text{if } 4 \mid y \end{cases}$$

and

$$V_{\frac{p-1}{4}}(6, -1) \equiv \begin{cases} 0 \pmod p & \text{if } 2 \parallel y, \\ \pm 2(-1)^{\frac{C-1}{4}+\frac{y}{4}}(\frac{x}{5}) \pmod p & \text{if } 4 \mid y \text{ and } x \equiv \pm C, \pm 3C \pmod 5. \end{cases}$$

Proof. Suppose $p = c^2 + d^2$ with $c, d \in \mathbb{Z}$ and $c \equiv 1 \pmod 4$. Clearly $2 \mid y$, $5 \mid cd$ and $5 \nmid Cx$. Thus $x \equiv \pm C$ or $\pm 3C \pmod 5$. Assume $x \equiv \varepsilon C, 3\varepsilon C \pmod 5$, where $\varepsilon \in \{1, -1\}$. As $(-1)^{\frac{x^2-1}{8}} = (-1)^{\frac{p-1-10y^2}{8}} = (-1)^{\frac{p-1}{8}+\frac{y}{2}}$, putting $m = 2, 10$ in Theorem 2.3 we have

$$2^{\frac{p-1}{4}} \equiv (-1)^{\frac{C^2-1}{8}} = (-1)^{\frac{C-1}{4}} \pmod p \quad \text{and} \quad 10^{\frac{p-1}{4}} \equiv (-1)^{\frac{p-1}{8}+\frac{y}{2}}\left(\frac{x}{5}\right) \pmod p.$$

Thus

$$5^{\frac{p-1}{4}} \equiv (-1)^{\frac{p-1}{8}+\frac{C-1}{4}+\frac{y}{2}}\left(\frac{x}{5}\right) \pmod p. \tag{8.5}$$

Now we prove the theorem by considering the following two cases.

Case 1. $x \equiv \pm c \pmod 5$. In this case, $5 \mid d$. As $c \equiv \pm x \equiv \pm\varepsilon C, \pm 3\varepsilon C \pmod 5$, by (6.9) and (6.12) we have $5^{\frac{p-1}{4}} \equiv 1 \pmod p$ and $5^{\frac{p-1}{8}} \equiv \pm\varepsilon \pmod p$. Hence from (8.5) we deduce $(-1)^{\frac{p-1}{8}} = (-1)^{\frac{C-1}{4}+\frac{y}{2}}(\frac{x}{5})$ and so $\pm(-5)^{\frac{p-1}{8}} \equiv (-1)^{\frac{p-1}{8}}\varepsilon = (-1)^{\frac{C-1}{4}+\frac{y}{2}}(\frac{x}{5})\varepsilon \pmod p$. Now applying Corollary 8.1 we see that

$$U_{\frac{p-1}{4}}(6, -1) \equiv \begin{cases} \pm(-5)^{\frac{p-1}{8}}\frac{y}{x} \equiv (-1)^{\frac{C-1}{4}+1}(\frac{x}{5})\varepsilon\frac{y}{x} \pmod p & \text{if } 2 \parallel y, \\ 0 \pmod p & \text{if } 4 \mid y \end{cases}$$

and

$$V_{\frac{p-1}{4}}(6, -1) \equiv \begin{cases} 0 \pmod p & \text{if } 2 \parallel y, \\ \pm 2(-1)^{\frac{y}{4}}(-5)^{\frac{p-1}{8}} \equiv 2(-1)^{\frac{y}{4}+\frac{C-1}{4}}(\frac{x}{5})\varepsilon \pmod p & \text{if } 4 \mid y. \end{cases}$$

Case 2. $x \equiv \pm d \pmod 5$. In this case, $5 \mid c$. As $d \equiv \pm x \equiv \pm\varepsilon C, \pm 3\varepsilon C \pmod 5$, by (6.9) and (6.11) we have $5^{\frac{p-1}{4}} \equiv -1 \pmod p$ and $5^{\frac{p-1}{8}} \equiv \pm\varepsilon\frac{c}{d} \pmod p$. Hence from (8.5) we deduce $(-1)^{\frac{p-1}{8}} = -(-1)^{\frac{C-1}{4}+\frac{y}{2}}(\frac{x}{5})$ and so $\pm(-5)^{\frac{p-1}{8}} \equiv (-1)^{\frac{C-1}{4}+\frac{y}{2}}(\frac{x}{5})\varepsilon\frac{d}{c} \pmod p$. Now applying Corollary 8.1 we see that

$$U_{\frac{p-1}{4}}(6, -1) \equiv \begin{cases} \pm(-5)^{\frac{p-1}{8}}\frac{cy}{dx} \equiv (-1)^{\frac{C-1}{4}+1}(\frac{x}{5})\varepsilon\frac{y}{x} \pmod p & \text{if } 2 \parallel y, \\ 0 \pmod p & \text{if } 4 \mid y \end{cases}$$

and

$$V_{\frac{p-1}{4}}(6, -1) \equiv \begin{cases} 0 \pmod p & \text{if } 2 \parallel y, \\ \pm 2(-1)^{\frac{y}{4}}(-5)^{\frac{p-1}{8}}\frac{c}{d} \equiv 2(-1)^{\frac{y}{4}+\frac{C-1}{4}}(\frac{x}{5})\varepsilon \pmod p & \text{if } 4 \mid y. \end{cases}$$

So the theorem is proved. □

Corollary 8.3. *Let $p \equiv 1, 9 \pmod{40}$ be a prime and hence $p = C^2 + 2D^2 = x^2 + 10y^2$ with $C, D, x, y \in \mathbb{Z}$. Suppose $C \equiv x \equiv 1 \pmod 4$, $y = 2^\beta y_0$ and $y_0 \equiv 1 \pmod 4$. Then*

$$(3+\sqrt{10})^{\frac{p-1}{4}} \equiv (-1)^{\frac{y}{2}}(3-\sqrt{10})^{\frac{p-1}{4}}$$
$$\equiv \begin{cases} \pm(-1)^{\frac{C-1}{4}+\frac{y}{4}}(\frac{x}{5}) \pmod p & \text{if } 4 \mid y \text{ and } x \equiv \pm C, \pm 3C \pmod 5, \\ \mp(-1)^{\frac{C-1}{4}}(\frac{x}{5})\frac{y}{x}\sqrt{10} \pmod p & \text{if } 2 \parallel y \text{ and } x \equiv \pm C, \pm 3C \pmod 5. \end{cases}$$

Proof. From (1.3) and (1.4) we know that

$$U_n(6,-1) = \frac{1}{2\sqrt{10}}\{(3+\sqrt{10})^n - (3-\sqrt{10})^n\},$$
$$V_n(6,-1) = (3+\sqrt{10})^n + (3-\sqrt{10})^n.$$

Thus $(3 \pm \sqrt{10})^{\frac{p-1}{4}} = \pm\sqrt{10}U_{\frac{p-1}{4}}(6,-1) + \frac{1}{2}V_{\frac{p-1}{4}}(6,-1)$. Now applying Theorem 8.5 we obtain the result. □

Corollary 8.4. *Let $p \equiv 1, 9 \pmod{40}$ be a prime and hence $p = C^2 + 2D^2 = x^2 + 10y^2$ with $C, D, x, y \in \mathbb{Z}$. Suppose $C \equiv x \equiv 1 \pmod 4$. Then*

$$p \mid U_{\frac{p-1}{8}}(6,-1) \iff (3+\sqrt{10})^{\frac{p-1}{4}} \equiv (-1)^{\frac{p-1}{8}} \pmod p$$
$$\iff 4 \mid y \quad \text{and} \quad (-1)^{\frac{D}{2}+\frac{y}{4}}\left(\frac{x}{5}\right)x \equiv C, 3C \pmod 5.$$

Proof. Note that $(-1)^{\frac{p-1}{8}+\frac{C-1}{4}} = (-1)^{\frac{p-1}{8}-\frac{C^2-1}{8}} = (-1)^{\frac{D}{2}}$. Applying Theorem 8.4 and Corollary 8.3 we obtain the result. □

9. Open conjectures

In the section we pose a lot of conjectures relating to the results in Sections 4–8.

In 1980 and 1984 Hudson and Williams proved the following result.

Theorem 9.1. *Let $p \equiv 1 \pmod{24}$ be a prime and hence $p = c^2 + d^2 = x^2 + 3y^2$ for some $c, d, x, y \in \mathbb{Z}$. Suppose $c \equiv 1 \pmod 4$.*

(i) (*See* [HW1].) *If $c \equiv \pm(-1)^{\frac{y}{4}} \pmod 3$, then $3^{\frac{p-1}{8}} \equiv \pm 1 \pmod p$.*
(ii) (*See* [H].) *If $d \equiv \pm(-1)^{\frac{y}{4}} \pmod 3$, then $3^{\frac{p-1}{8}} \equiv \pm\frac{d}{c} \pmod p$.*

Hudson and Williams proved Theorem 9.1(i) by using the cyclotomic numbers of order 12, and Hudson proved Theorem 9.1(ii) using the Jacobi sums of order 24.

Now we pose some conjectures similar to Theorem 9.1.

Conjecture 9.1. *Let $p \equiv 13 \pmod{24}$ be a prime and hence $p = c^2 + d^2 = x^2 + 3y^2$ for some $c, d, x, y \in \mathbb{Z}$. Suppose $c \equiv 1 \pmod 4$, $x = 2^\alpha x_0$, $y = 2^\beta y_0$ and $x_0 \equiv y_0 \equiv 1 \pmod 4$. Then*

$$3^{\frac{p-5}{8}} \equiv \begin{cases} \pm\frac{y}{x} \pmod p & \text{if } x \equiv \pm c \pmod 3, \\ \mp\frac{dy}{cx} \pmod p & \text{if } x \equiv \pm d \pmod 3. \end{cases}$$

Conjecture 9.1 has been checked for all primes $p < 3000$.

Conjecture 9.2. *Let $p \equiv 1, 9, 25 \pmod{28}$ be a prime and hence $p = c^2 + d^2 = x^2 + 7y^2$ for some $c, d, x, y \in \mathbb{Z}$. Suppose $c \equiv 1 \pmod 4$, $x = 2^\alpha x_0$, $y = 2^\beta y_0$ and $x_0 \equiv y_0 \equiv 1 \pmod 4$.*

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

$$7^{\frac{p-1}{8}} \equiv \begin{cases} -(-1)^{\frac{y}{4}} \pmod p & \text{if } 7 \mid c, \\ (-1)^{\frac{y}{4}} \pmod p & \text{if } 7 \mid d, \\ \mp(-1)^{\frac{y}{4}} \frac{d}{c} \pmod p & \text{if } c \equiv \pm d \pmod 7. \end{cases}$$

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

$$7^{\frac{p-5}{8}} \equiv \begin{cases} -\frac{y}{x} \pmod p & \text{if } 7 \mid c, \\ \frac{y}{x} \pmod p & \text{if } 7 \mid d, \\ \mp\frac{dy}{cx} \pmod p & \text{if } c \equiv \pm d \pmod 7. \end{cases}$$

Conjecture 9.2 has been checked for all primes $p < 5000$.

Conjecture 9.3. *Let $p \equiv 1 \pmod 4$ be a prime such that $p = c^2 + d^2 = x^2 + 11y^2$ with $c, d, x, y \in \mathbb{Z}$ and $11 \mid cd$. Suppose $c \equiv 1 \pmod 4$, $x = 2^\alpha x_0$, $y = 2^\beta y_0$ and $x_0 \equiv y_0 \equiv 1 \pmod 4$.*

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

$$11^{\frac{p-1}{8}} \equiv \begin{cases} \pm(-1)^{\frac{y}{4}} \pmod p & \text{if } x \equiv \pm c \pmod{11}, \\ \pm(-1)^{\frac{y}{4}} \frac{d}{c} \pmod p & \text{if } x \equiv \pm d \pmod{11}. \end{cases}$$

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

$$11^{\frac{p-5}{8}} \equiv \begin{cases} \pm\frac{y}{x} \pmod p & \text{if } x \equiv \pm c \pmod{11}, \\ \pm\frac{dy}{cx} \pmod p & \text{if } x \equiv \pm d \pmod{11}. \end{cases}$$

Conjecture 9.3 has been checked for all primes $p < 15000$.

For a given nonzero integer $m = 2^r m_0$ $(2 \nmid m_0)$ we recall that m_0 is called the odd part of m.

Conjecture 9.4. *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 $c \equiv 1 \pmod 4$ and all the odd parts of d, x, y are numbers of the form $4k + 1$.*

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

$$U_{\frac{p-1}{4}}(b, -1) \equiv \begin{cases} (-1)^{\frac{d}{4}} \frac{2y}{x} \pmod p & \text{if } 2 \parallel x \text{ and } b \equiv 1, 3 \pmod 8, \\ -(-1)^{\frac{d}{4}} \frac{2y}{x} \pmod p & \text{if } 2 \parallel x \text{ and } b \equiv 5, 7 \pmod 8, \\ \frac{2dy}{cx} \pmod p & \text{if } 2 \parallel y. \end{cases}$$

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

$$V_{\frac{p-1}{4}}(b, -1) \equiv \begin{cases} 2(-1)^{\frac{d+y}{4}} \pmod p & \text{if } 4 \mid y, \\ -2(-1)^{\frac{x}{4}} \frac{d}{c} \pmod p & \text{if } 4 \mid x \text{ and } b \equiv 1, 3 \pmod 8, \\ 2(-1)^{\frac{x}{4}} \frac{d}{c} \pmod p & \text{if } 4 \mid x \text{ and } b \equiv 5, 7 \pmod 8. \end{cases}$$

Conjecture 9.4 has been checked for $b < 60$ and $p < 20000$. When $p \equiv 1 \pmod 8$, $b = 1, 3$ 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 [L2, Conjecture 4].

By (1.3) and (1.4), Conjecture 9.4 is equivalent to the following conjecture.

Conjecture 9.5. *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 $c \equiv 1 \pmod 4$ and all the odd parts of d, x, y are numbers of the form $4k + 1$.*

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

$$\left(\frac{b + \frac{cx}{dy}}{2}\right)^{\frac{p-1}{4}} \equiv -\left(\frac{b - \frac{cx}{dy}}{2}\right)^{\frac{p-1}{4}} \equiv \begin{cases} -(-1)^{\frac{d}{4}} \frac{d}{c} \pmod p & \text{if } 2 \parallel x \text{ and } b \equiv 1, 3 \pmod 8, \\ (-1)^{\frac{d}{4}} \frac{d}{c} \pmod p & \text{if } 2 \parallel x \text{ and } b \equiv 5, 7 \pmod 8, \\ 1 \pmod p & \text{if } 2 \parallel y. \end{cases}$$

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

$$\left(\frac{b + \frac{cx}{dy}}{2}\right)^{\frac{p-1}{4}} \equiv \left(\frac{b - \frac{cx}{dy}}{2}\right)^{\frac{p-1}{4}} \equiv \begin{cases} (-1)^{\frac{d+y}{4}} \pmod p & \text{if } 4 \mid y, \\ -(-1)^{\frac{x}{4}} \frac{d}{c} \pmod p & \text{if } 4 \mid x \text{ and } b \equiv 1, 3 \pmod 8, \\ (-1)^{\frac{x}{4}} \frac{d}{c} \pmod p & \text{if } 4 \mid x \text{ and } b \equiv 5, 7 \pmod 8. \end{cases}$$

For $t \in \mathbb{Z}$ let $\delta(t) = 1$ or -1 according as $8 \mid t$ or not. From Conjecture 9.4 and Theorem 6.3 (or Theorem 6.2 with $k = 1$) we deduce:

Conjecture 9.6. *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 $c \equiv 1 \pmod 4$ and all the odd parts of d, x, y are numbers of the form $4k + 1$.*

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

$$(b^2 + 4)^{\frac{p-1}{8}} \equiv \begin{cases} \pm(-1)^{\frac{b-1}{2} + \frac{d}{4}} \delta(y) \frac{d}{c} \pmod p & \text{if } \left(\frac{(2c+bd)/x}{b+2i}\right)_4 = \pm 1, \\ \pm(-1)^{\frac{b-1}{2} + \frac{d}{4}} \delta(y) \pmod p & \text{if } \left(\frac{(2c+bd)/x}{b+2i}\right)_4 = \pm i. \end{cases}$$

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

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

We note that $(\frac{(2c+bd)/x}{b+2i})_4$ depends only on $(2c + bd)/x \pmod{b^2 + 4}$.

Taking $b = 1$ in Conjecture 9.6 we deduce:

Conjecture 9.7. *Let $p \equiv 1, 9 \pmod{20}$ be a prime and hence $p = c^2 + d^2 = x^2 + 5y^2$ for some $c, d, x, y \in \mathbb{Z}$. Suppose $c \equiv 1 \pmod 4$ and all the odd parts of d, x, y are congruent to 1 modulo 4.*

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

$$5^{\frac{p-1}{8}} \equiv \begin{cases} \pm(-1)^{\frac{d}{4}}\delta(y) \pmod p & \text{if } x \equiv \pm c \pmod 5, \\ \pm(-1)^{\frac{d}{4}}\delta(y)\frac{d}{c} \pmod p & \text{if } x \equiv \pm d \pmod 5. \end{cases}$$

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

$$5^{\frac{p-5}{8}} \equiv \begin{cases} \pm\delta(x)\frac{dy}{cx} \pmod p & \text{if } x \equiv \pm c \pmod 5, \\ \mp\delta(x)\frac{y}{x} \pmod p & \text{if } x \equiv \pm d \pmod 5. \end{cases}$$

Conjecture 9.7 has been checked for all primes $p < 2500$.

Let $p \equiv 1 \pmod{40}$ be a prime and let g be a primitive root $\pmod p$. For $h, k \in \{0, 1, \dots, 19\}$ let $(h,k)_{20}$ be the number of integers n $(1 \leqslant n < p-1)$ such that $n \equiv g^h \pmod{20}$ and $n+1 \equiv g^k \pmod{20}$. Suppose $5 \equiv g^m \pmod p$ for some integer m. Then $5^{\frac{p-1}{8}} \equiv g^{\frac{p-1}{8}m} \pmod p$ and so $5^{\frac{p-1}{8}} \equiv 1 \pmod p$ if and only if $8 \mid m$. By [HW1, Theorem 1] we have

$$m \equiv 2\sum_{i=1}^{3} i \sum_{j=1}^{2}\sum_{r=0}^{4}\sum_{s=0}^{3}(i+4r, j+5s)_{20} + \frac{16(p-1)}{40} \pmod 8.$$

Thus, it is possible to prove Conjecture 9.7(i) in the case of $p \equiv 1 \pmod{40}$ by using the cyclotomic numbers $(h,k)_{20}$ given by Muskat and Whiteman [MW].

Now we pose another conjecture for $5^{\frac{p-1}{8}} \pmod p$.

Conjecture 9.8. *Let* $p \equiv 1, 9 \pmod{40}$ *be a prime and hence* $p = c^2 + d^2 = x^2 + 10y^2$ *for some* $c, d, x, y \in \mathbb{Z}$. *Suppose* $c \equiv x \equiv 1 \pmod 4$. *Then*

$$5^{\frac{p-1}{8}} \equiv \begin{cases} \pm(-1)^{\frac{d}{4}+\frac{x-1}{4}}\frac{d}{c} \pmod p & \text{if } x \equiv \pm d \pmod 5, \\ \pm(-1)^{\frac{d}{4}+\frac{x-1}{4}} \pmod p & \text{if } x \equiv \pm c \pmod 5. \end{cases}$$

Taking $b = 3$ in Conjecture 9.6 we deduce:

Conjecture 9.9. *Let* $p \equiv 1, 9, 17, 25, 29, 49 \pmod{52}$ *be a prime and hence* $p = c^2 + d^2 = x^2 + 13y^2$ *for some* $c, d, x, y \in \mathbb{Z}$. *Suppose* $c \equiv 1 \pmod 4$ *and all the odd parts of* d, x, y *are congruent to* 1 *modulo* 4.

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

$$13^{\frac{p-1}{8}} \equiv \begin{cases} \mp(-1)^{\frac{d}{4}}\delta(y)\frac{d}{c} \pmod p & \text{if } \frac{2c+3d}{x} \equiv \pm 1, \pm 3, \pm 9 \pmod{13}, \\ \pm(-1)^{\frac{d}{4}}\delta(y) \pmod p & \text{if } \frac{2c+3d}{x} \equiv \pm 2, \pm 5, \pm 6 \pmod{13}. \end{cases}$$

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

$$13^{\frac{p-5}{8}} \equiv \begin{cases} \pm\delta(x)\frac{y}{x} \pmod p & \text{if } \frac{2c+3d}{x} \equiv \pm 1, \pm 3, \pm 9 \pmod{13}, \\ \pm\delta(x)\frac{dy}{cx} \pmod p & \text{if } \frac{2c+3d}{x} \equiv \pm 2, \pm 5, \pm 6 \pmod{13}. \end{cases}$$

From Conjecture 9.4 and (1.5) we deduce:

Conjecture 9.10. *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* $2 \mid d$. *Then* $p \mid U_{\frac{p-1}{8}}(b, -1)$ *if and only if* $4 \mid y$ *and* $(-1)^{\frac{d+y}{4}} = (-1)^{\frac{p-1}{8}}$.

Conjecture 9.11. *Let $p \equiv 1 \pmod 4$ be a prime, $b \in \mathbb{Z}$, $b \equiv 4 \pmod 8$, $p \ne b^2/4+1$ and $p = c^2+d^2 = x^2+(1+b^2/4)y^2$ for some $c, d, x, y \in \mathbb{Z}$. Suppose $c \equiv 1 \pmod 4$ and all the odd parts of d, x, y are numbers of the form $4k+1$. Then*

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

and

$$V_{\frac{p-1}{4}}(b,-1) \equiv \begin{cases} 2(-1)^{\frac{d}{4}+\frac{y}{4}} \pmod p & \textit{if } 4 \mid y, \\ 2(-1)^{\frac{b-4}{8}+\frac{x}{4}}\frac{d}{c} \pmod p & \textit{if } 4 \mid x, \\ 0 \pmod p & \textit{if } 4 \nmid xy. \end{cases}$$

Conjecture 9.11 has been checked for $b \leqslant 100$ and $p < 20000$. When $p \equiv 1 \pmod 8$, $b = 12$ and $4 \mid y$, the conjecture $V_{\frac{p-1}{4}}(12,-1) \equiv 2(-1)^{\frac{d+y}{4}} \pmod p$ is equivalent to a conjecture of E. Lehmer. See [L2, Conjecture 4].

From Conjecture 9.11 and Theorem 7.3 we deduce:

Conjecture 9.12. *Let $p \equiv 1 \pmod 4$ be a prime, $a \in \mathbb{Z}$, $2 \nmid a$, $p \ne 4a^2+1$ and $p = c^2+d^2 = x^2+(4a^2+1)y^2$ for some $c, d, x, y \in \mathbb{Z}$. Suppose $c \equiv 1 \pmod 4$ and all the odd parts of d, x, y are numbers of the form $4k+1$.*

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

$$\left(4a^2+1\right)^{\frac{p-1}{8}} \equiv \begin{cases} \pm(-1)^{\frac{d}{4}}\delta(y)\frac{d}{c} \pmod p & \textit{if } \left(\frac{(d-2ac)/x}{1-2ai}\right)_4 = \pm 1, \\ \pm(-1)^{\frac{d}{4}}\delta(y) \pmod p & \textit{if } \left(\frac{(d-2ac)/x}{1-2ai}\right)_4 = \pm i. \end{cases}$$

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

$$\left(4a^2+1\right)^{\frac{p-5}{8}} \equiv \begin{cases} \mp\delta(x)\frac{y}{x} \pmod p & \textit{if } \left(\frac{(d-2ac)/x}{1-2ai}\right)_4 = \pm 1, \\ \pm\delta(x)\frac{dy}{cx} \pmod p & \textit{if } \left(\frac{(d-2ac)/x}{1-2ai}\right)_4 = \pm i. \end{cases}$$

From Corollary 7.1 and Conjecture 9.11 (with $b = 12$) we deduce:

Conjecture 9.13. *Let p be a prime such that $p \equiv 1, 9, 21, 25, 33, 41, 49, 53, 65, 73, 77, 81, 85, 101, 121, 137, 141, 145 \pmod{148}$ and hence $p = c^2+d^2 = x^2+37y^2$ for some $c, d, x, y \in \mathbb{Z}$. Suppose $c \equiv 1 \pmod 4$ and all the odd parts of d, x, y are numbers of the form $4k+1$.*

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

$$37^{\frac{p-1}{8}} \equiv \begin{cases} \pm(-1)^{\frac{d}{4}}\delta(y)\frac{d}{c} \pmod p & \textit{if } \frac{d-6c}{x} \equiv \pm 1, \pm 7, \pm 9, \pm 10, \\ & \qquad \pm 12, \pm 16, \pm 26, \pm 33, \pm 34 \pmod{37}, \\ \pm(-1)^{\frac{d}{4}}\delta(y) \pmod p & \textit{if } \frac{d-6c}{x} \equiv \pm 2, \pm 14, \pm 15, \pm 18, \\ & \qquad \pm 20, \pm 24, \pm 29, \pm 31, \pm 32 \pmod{37}. \end{cases}$$

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

$$37^{\frac{p-5}{8}} \equiv \begin{cases} \mp\delta(x)\frac{y}{x} \pmod p & \text{if } \frac{d-6c}{x} \equiv \pm 1, \pm 7, \pm 9, \pm 10, \\ & \quad \pm 12, \pm 16, \pm 26, \pm 33, \pm 34 \pmod{37}, \\ \pm\delta(x)\frac{dy}{cx} \pmod p & \text{if } \frac{d-6c}{x} \equiv \pm 2, \pm 14, \pm 15, \pm 18, \\ & \quad \pm 20, \pm 24, \pm 29, \pm 31, \pm 32 \pmod{37}. \end{cases}$$

Conjecture 9.14. *Let* $p \equiv 1 \pmod 4$ *be a prime,* $b \in \mathbb{Z}$, $8 \mid b$, $p \neq b^2/4 + 1$ *and* $p = c^2 + d^2 = x^2 + (1 + b^2/4)y^2$ *for some* $c, d, x, y \in \mathbb{Z}$. *Suppose* $c \equiv 1 \pmod 4$ *and all the odd parts of* d, x, y *are numbers of the form* $4k + 1$. *Then*

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

and

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

Conjecture 9.14 has been checked for $b < 100$ and $p < 20000$.

From Conjecture 9.14 and Theorem 7.3 we deduce:

Conjecture 9.15. *Let* $p \equiv 1 \pmod 4$ *be a prime,* $a \in \mathbb{Z}$ *and* $2 \mid a$. *Suppose* $4a^2 + 1 \neq p$ *and* $p = c^2 + d^2 = x^2 + (4a^2 + 1)y^2$ *with* $c, d, x, y \in \mathbb{Z}$ *and* $c \equiv 1 \pmod 4$. *Suppose that all the odd parts of* d, x, y *are numbers of the form* $4k + 1$.

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

$$(4a^2+1)^{\frac{p-1}{8}} \equiv \begin{cases} \pm(-1)^{\frac{d}{4}+\frac{xy}{4}} \pmod p & \text{if } \left(\frac{(d-2ac)/x}{1-2ai}\right)_4 = \pm 1, \\ \pm(-1)^{\frac{d}{4}+\frac{xy}{4}}\frac{c}{d} \pmod p & \text{if } \left(\frac{(d-2ac)/x}{1-2ai}\right)_4 = \pm i. \end{cases}$$

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

$$(4a^2+1)^{\frac{p-5}{8}} \equiv \begin{cases} \pm(-1)^x\frac{dy}{cx} \pmod p & \text{if } \left(\frac{(d-2ac)/x}{1-2ai}\right)_4 = \pm 1, \\ \pm(-1)^x\frac{y}{x} \pmod p & \text{if } \left(\frac{(d-2ac)/x}{1-2ai}\right)_4 = \pm i. \end{cases}$$

Taking $a = -2$ in Conjecture 9.15 we have:

Conjecture 9.16. *Let* $p \equiv 1 \pmod 4$ *be a prime and* $p = c^2 + d^2 = x^2 + 17y^2$ *for some* $c, d, x, y \in \mathbb{Z}$. *Suppose* $c \equiv 1 \pmod 4$ *and all the odd parts of* d, x, y *are numbers of the form* $4k + 1$.

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

$$17^{\frac{p-1}{8}} \equiv \begin{cases} -(-1)^{\frac{d}{4}+\frac{xy}{4}}\frac{d}{c} \pmod p & \text{if } 4c + d \equiv \pm 6x, \pm 7x \pmod{17}, \\ (-1)^{\frac{d}{4}+\frac{xy}{4}}\frac{d}{c} \pmod p & \text{if } 4c + d \equiv \pm 3x, \pm 5x \pmod{17}, \\ (-1)^{\frac{d}{4}+\frac{xy}{4}} \pmod p & \text{if } 4c + d \equiv \pm x, \pm 4x \pmod{17}, \\ -(-1)^{\frac{d}{4}+\frac{xy}{4}} \pmod p & \text{if } 4c + d \equiv \pm 2x, \pm 8x \pmod{17}. \end{cases}$$

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

$$17^{\frac{p-5}{8}} \equiv \begin{cases} (-1)^x \frac{y}{x} \pmod p & \textit{if } 4c+d \equiv \pm 6x, \pm 7x \pmod{17}, \\ -(-1)^x \frac{y}{x} \pmod p & \textit{if } 4c+d \equiv \pm 3x, \pm 5x \pmod{17}, \\ (-1)^x \frac{dy}{cx} \pmod p & \textit{if } 4c+d \equiv \pm x, \pm 4x \pmod{17}, \\ -(-1)^x \frac{dy}{cx} \pmod p & \textit{if } 4c+d \equiv \pm 2x, \pm 8x \pmod{17}. \end{cases}$$

Conjecture 9.16 has been checked for all primes $p < 5000$.

Conjecture 9.17. *Let* $p \equiv 1 \pmod 4$ *be a prime,* $b \in \mathbb{Z}$, $b \equiv 2 \pmod 4$, $p \ne b^2/4+1$ *and* $p = c^2+d^2 = x^2+(1+b^2/4)y^2$ *for some* $c, d, x, y \in \mathbb{Z}$. *Suppose* $c \equiv 1 \pmod 4$, $x = 2^{\alpha}x_0$, $y = 2^{\beta}y_0$ *and* $x_0 \equiv y_0 \equiv 1 \pmod 4$. *Then*

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

and

$$V_{\frac{p-1}{4}}(b,-1) \equiv \begin{cases} 0 \pmod p & \textit{if } 2 \parallel y, \\ 2(-1)^{\frac{d}{4}+\frac{y}{4}} \pmod p & \textit{if } 4 \mid y. \end{cases}$$

Conjecture 9.17 has been checked for $b < 100$ and $p < 20{,}000$.

From Conjecture 9.17 and Theorem 8.3(i) we deduce:

Conjecture 9.18. *Let* $a \in \mathbb{Z}$ *be odd, and let* $p \equiv 1 \pmod 8$ *be a prime such that* $p = c^2+d^2 = x^2+(a^2+1)y^2$ *with* $c, d, x, y \in \mathbb{Z}$ *and* $a \equiv c \equiv x \equiv 1 \pmod 4$. *Then*

$$\left(\frac{a^2+1}{2}\right)^{\frac{p-1}{8}} \equiv \begin{cases} \pm(-1)^{\frac{d}{4}+\frac{x-1}{4}}(d/c)^{(1-(-1)^{\frac{a-1}{4}})/2} \pmod p & \textit{if } \left(\frac{(\frac{1-a}{2}c-\frac{1+a}{2}d)/x}{\frac{1+a}{2}+\frac{1-a}{2}i}\right)_4 = \pm 1, \\ \pm(-1)^{\frac{d}{4}+\frac{x-1}{4}}(d/c)^{1+(1-(-1)^{\frac{a-1}{4}})/2} \pmod p & \textit{if } \left(\frac{(\frac{1-a}{2}c-\frac{1+a}{2}d)/x}{\frac{1+a}{2}+\frac{1-a}{2}i}\right)_4 = \pm i. \end{cases}$$

We note that $(-1)^{\frac{x-1}{4}} = (-1)^{\frac{p-1}{8}+\frac{y}{2}}$.

Taking $a = -3$ in Conjecture 9.18 we deduce Conjecture 9.8.

From Conjectures 9.11, 9.14, 9.17 and (1.5) we have:

Conjecture 9.19. *Let* $p \equiv 1 \pmod 8$ *be a prime. Let* $b \in \mathbb{Z}$ *with* $2 \mid b$ *and* $1+b^2/4 \ne p$. *Suppose* $p = c^2+d^2 = x^2+(1+b^2/4)y^2$ *with* $c, d, x, y \in \mathbb{Z}$ *and* $2 \mid d$. *Then*

$$p \mid U_{\frac{p-1}{8}}(b,-1) \iff \begin{cases} 4 \mid y \textit{ and } (-1)^{\frac{d}{4}+\frac{y}{4}} = (-1)^{\frac{p-1}{8}} & \textit{if } 8 \nmid b, \\ (-1)^{\frac{d}{4}+\frac{xy}{4}+\frac{b}{8}y} = (-1)^{\frac{p-1}{8}} & \textit{if } 8 \mid b. \end{cases}$$

Conjecture 9.20. *(See [S5, Conjecture 5.2].) Let* $p \equiv 3, 7 \pmod{20}$ *be a prime, and hence* $2p = x^2+5y^2$ *for some integers* x *and* y. *Then*

$$F_{\frac{p+1}{4}} \equiv \begin{cases} 2(-1)^{[\frac{p-5}{10}]} \cdot 10^{\frac{p-3}{4}} \pmod p & \textit{if } y \equiv \pm\frac{p-1}{2} \pmod 8, \\ -2(-1)^{[\frac{p-5}{10}]} \cdot 10^{\frac{p-3}{4}} \pmod p & \textit{if } y \not\equiv \pm\frac{p-1}{2} \pmod 8. \end{cases}$$

It is well known that $L_n = F_{n+1} + F_{n-1}$ and $F_nL_n = F_{2n}$. From [SS, Corollary 2(iii)] we have

$$F_{\frac{p+1}{4}} L_{\frac{p+1}{4}} = F_{\frac{p+1}{2}} \equiv 2(-1)^{[\frac{p-5}{10}]} \cdot 5^{\frac{p-3}{4}} \pmod p.$$

Thus the above conjecture is equivalent to

$$L_{\frac{p+1}{4}} \equiv \begin{cases} (-2)^{\frac{p+1}{4}} \pmod p & \text{if } y \equiv \pm\frac{p-1}{2} \pmod 8, \\ -(-2)^{\frac{p+1}{4}} \pmod p & \text{if } y \not\equiv \pm\frac{p-1}{2} \pmod 8. \end{cases} \tag{9.1}$$

We have checked (9.1) for all primes $p < 3000$.

As

$$2\left(\frac{1+\sqrt{5}}{2}\right)^{\frac{p+1}{4}} = L_{\frac{p+1}{4}} + F_{\frac{p+1}{4}}\sqrt{5},$$

by the conjecture we have

$$\begin{aligned} (1+\sqrt{5})^{\frac{p+1}{4}} &= 2^{\frac{p-3}{4}}\left(L_{\frac{p+1}{4}} + F_{\frac{p+1}{4}}\sqrt{5}\right) \\ &\equiv \left(\frac{2}{\frac{p-1}{2}y}\right) 2^{\frac{p-3}{4}}\left((-2)^{\frac{p+1}{4}} + 2(-1)^{[\frac{p-5}{10}]} \cdot 10^{\frac{p-3}{4}}\sqrt{5}\right) \\ &= \left(\frac{2}{\frac{p-1}{2}y}\right)\left((-1)^{\frac{p+1}{4}} 2^{\frac{p-1}{2}} + (-1)^{[\frac{p-5}{10}]} 2^{\frac{p-1}{2}} \cdot 5^{\frac{p-3}{4}}\sqrt{5}\right) \\ &\equiv \left(\frac{2}{\frac{p-1}{2}y}\right)\left(1 + (-1)^{[\frac{p-5}{10}]}\left(\frac{2}{p}\right) 5^{\frac{p-3}{4}}\sqrt{5}\right) \pmod p. \end{aligned}$$

From this we deduce the following conjecture equivalent to Conjecture 9.20.

Conjecture 9.21. *Let $p \equiv 3, 7 \pmod{20}$ be a prime and so $2p = x^2 + 5y^2$ for some integers x and y. Then*

$$(-1)^{\frac{y^2-1}{8}}(1+\sqrt{5})^{\frac{p+1}{4}} \equiv \begin{cases} 1 + 5^{\frac{p-3}{4}}\sqrt{5} \pmod p & \textit{if } p \equiv 3, 47 \pmod{80}, \\ -1 - 5^{\frac{p-3}{4}}\sqrt{5} \pmod p & \textit{if } p \equiv 7, 43 \pmod{80}, \\ 1 - 5^{\frac{p-3}{4}}\sqrt{5} \pmod p & \textit{if } p \equiv 63, 67 \pmod{80}, \\ -1 + 5^{\frac{p-3}{4}}\sqrt{5} \pmod p & \textit{if } p \equiv 23, 27 \pmod{80}. \end{cases}$$

Added remark. In 2007 Constantin-Nicolae Beli informed the author he could prove (1.8) independently by using class field theory and showed me how to prove Conjecture 9.20 using class field theory. Thus Conjecture 9.21 is also true. In the November of 2007 the author formulated the following general conjecture including many of the above conjectures.

Conjecture 9.22. *Let p be a prime of the form $4k+1$, $a, b \in \mathbb{Z}$, $2 \mid a$, $(a, b) = 1$, $p \ne a^2 + b^2$ and $p = c^2 + d^2 = x^2 + (a^2+b^2)y^2$, where $c, d, x, y \in \mathbb{Z}$, $c \equiv 1 \pmod 4$ and all the odd parts of d, x, y are of the form $4k+1$. Suppose $(\frac{(ac+bd)/x}{b+ai})_4 = i^r$.*

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

$$\left(a^2+b^2\right)^{\frac{p-1}{8}} \equiv \begin{cases} (-1)^{\frac{b-1}{2}+\frac{d}{4}}\delta(y)(c/d)^{r-1} \pmod p & \textit{if } 2 \parallel a, \\ (-1)^{\frac{d}{4}+\frac{xy}{4}}(c/d)^r \pmod p & \textit{if } 4 \mid a. \end{cases}$$

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

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

References

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

[E] R.J. Evans, Residuacity of primes, Rocky Mountain J. Math. 19 (1989) 1069–1081.

[H] R.H. Hudson, Diophantine determinations of $3^{(p-1)/8}$ and $5^{(p-1)/4}$, Pacific J. Math. 111 (1984) 49–55.

[HW1] R.H. Hudson, K.S. Williams, Some new residuacity criteria, Pacific J. Math. 91 (1980) 135–143.

[HW2] R.H. Hudson, K.S. Williams, An application of a formula of Western to the evaluation of certain Jacobsthal sums, Acta Arith. 41 (1982) 261–276.

[HW3] R.H. Hudson, K.S. Williams, Extensions of theorems of Cunningham–Aigner and Hasse–Evans, Pacific J. Math. 104 (1983) 111–132.

[IR] K. Ireland, M. Rosen, A Classical Introduction to Modern Number Theory, second ed., Springer, New York, 1990.

[L1] E. Lehmer, On Euler's criterion, J. Austral. Math. Soc. 1 (1959) 64–70.

[L2] E. Lehmer, On the quartic character of quadratic units, J. Reine Angew. Math. 268/269 (1974) 294–301.

[MW] J.B. Muskat, A.L. Whiteman, The cyclotomic numbers of order twenty, Acta Arith. 17 (1970) 185–216.

[S1] Z.H. Sun, Notes on quartic residue symbol and rational reciprocity laws, J. Nanjing Univ. Math. Biquarterly 9 (1992) 92–101.

[S2] Z.H. Sun, The combinatorial sum $\sum_{\substack{k=0\\ k\equiv r \pmod m}}^{n} \binom{n}{k}$ and its applications in number theory II, J. Nanjing Univ. Math. Biquarterly 10 (1993) 105–118.

[S3] Z.H. Sun, On the theory of cubic residues and nonresidues, Acta Arith. 84 (1998) 291–335.

[S4] Z.H. Sun, Supplements to the theory of quartic residues, Acta Arith. 97 (2001) 361–377.

[S5] Z.H. Sun, Values of Lucas sequences modulo primes, Rocky Mountain J. Math. 33 (2003) 1123–1145.

[S6] Z.H. Sun, Quartic residues and binary quadratic forms, J. Number Theory 113 (2005) 10–52.

[S7] Z.H. Sun, On the quadratic character of quadratic units, J. Number Theory 128 (2008) 1295–1335.

[SS] Z.H. Sun, Z.W. Sun, Fibonacci numbers and Fermat's last theorem, Acta Arith. 60 (1992) 371–388.

[P] P. Pollack, Rational(!) cubic and biquadratic reciprocity, Lecture Note, 2005, http://www.math.dartmouth.edu/~ppollack/reci.pdf.