Journal of Number Theory 128(2008), 1295-1335.

ON THE QUADRATIC CHARACTER OF QUADRATIC UNITS

ZHI-Hong Sun

Department of Mathematics, Huaiyin Teachers College,
Huaian, Jiangsu 223001, PR China
E-mail: szh6174@yahoo.com
Homepage: http://www.hytc.edu.cn/xsjl/szh

Abstract. Let $p \equiv 1 \pmod 4$ be a prime. Let $a, b \in \mathbb{Z}$ with $p \nmid a(a^2+b^2)$. In the paper we mainly determine $(\frac{b+\sqrt{a^2+b^2}}{2})^{\frac{p-1}{2}} \pmod p$ by assuming $p = c^2+d^2$ or $p = Ax^2+2Bxy+Cy^2$ with $AC-B^2 = a^2+b^2$. As an application we obtain simple criteria for ε_D to be a quadratic residue $\pmod p$, where $D > 1$ is a squarefree integer such that D is a quadratic residue of p, ε_D is the fundamental unit of the quadratic field $\mathbb{Q}(\sqrt{D})$ with negative norm. We also establish the congruences for $U_{(p\pm1)/2} \pmod p$ and obtain a general criterion for $p \mid U_{(p-1)/4}$, where $\{U_n\}$ is the Lucas sequence defined by $U_0 = 0,\ U_1 = 1$ and $U_{n+1} = bU_n + k^2U_{n-1}\ (n \ge 1)$.

MSC: Primary 11A15, Secondary 11B39, 11A07, 11E25, 11E16
Keywords: Quadratic residue; Fundamental unit; Congruence; Lucas sequence; Jacobi symbol

1. Introduction.

Let $\mathbb{Z}$ be the set of integers, $i = \sqrt{-1}$ and $\mathbb{Z}[i] = \{a+bi \mid a, b \in \mathbb{Z}\}$. For $\pi = a+bi \in \mathbb{Z}[i]$ the norm of π is given by $N\pi = \pi\bar{\pi} = a^2+b^2$, where $\bar{\pi}$ means the complex conjugate of π. If $2 \mid b$ and $a+b \equiv 1 \pmod 4$, we say that π is primary. If π or $-\pi$ is primary in $\mathbb{Z}[i]$, it is known that (see [IR, p. 121]) $\pi = \pm\pi_1\cdots\pi_r$, where $\pi_1, \dots, \pi_r$ are primary irreducibles. For $\alpha \in \mathbb{Z}[i]$ the quartic Jacobi symbol $\left(\frac{\alpha}{\pi}\right)_4$ is defined by

$$\left(\frac{\alpha}{\pi}\right)_4 = \left(\frac{\alpha}{\pi_1}\right)_4 \cdots \left(\frac{\alpha}{\pi_r}\right)_4,$$

where $\left(\frac{\alpha}{\pi_s}\right)_4$ is the quartic residue character of α modulo π_s given by

$$\left(\frac{\alpha}{\pi_s}\right)_4 = \begin{cases} 0 & \text{if } \pi_s \mid \alpha, \\ i^r & \text{if } \alpha^{(N\pi_s-1)/4} \equiv i^r \pmod{\pi_s}. \end{cases}$$

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

If $a+bi$ is primary in $\mathbb{Z}[i]$, it is known that

$$\Big(\frac{i}{a+bi}\Big)_4 = i^{\frac{a^2+b^2-1}{4}} = i^{\frac{1-a}{2}} \quad \text{and} \quad \Big(\frac{1+i}{a+bi}\Big)_4 = i^{\frac{a-b-b^2-1}{4}}.$$

If $a+bi$ and $c+di$ are relatively prime primary elements of $\mathbb{Z}[i]$, then we have the following general law of biquadratic reciprocity:

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

For more properties of the quartic Jacobi symbol one may consult [IR, pp. 122-123, 311] and [Su6, (2.1)-(2.8)].

For any odd number $m>1$ and $a\in\mathbb{Z}$ let $(\frac{a}{m})$ be the (quadratic) Jacobi symbol. For our convenience we also define $(\frac{a}{-m}) = (\frac{a}{m})$ and $\big(\frac{a}{1}\big) = \big(\frac{a}{-1}\big) = 1$. Then for any two odd numbers m and n with $m,n\neq\pm1$ we have the following general quadratic reciprocity law: $(\frac{m}{n}) = (-1)^{\frac{m-1}{2}\cdot\frac{n-1}{2}}(\frac{n}{m})$. If $m>1$ is odd, $a,b,x\in\mathbb{Z}$, $ax\equiv b \pmod m$ and a is coprime to m, we define $\big(\frac{b/a}{m}\big) = \big(\frac{x}{m}\big)$. Hence $\big(\frac{b/a}{m}\big) = \big(\frac{a}{m}\big)\big(\frac{b}{m}\big)$.

Let $D>1$ be a squarefree integer, and $\varepsilon_D = (m+n\sqrt{D})/2$ be the fundamental unit of the quadratic field $\mathbb{Q}(\sqrt{D})$ ($\mathbb{Q}$ is the set of rational numbers). Suppose that $p\equiv 1 \pmod 4$ is a prime such that $(\frac{D}{p}) = 1$. As $\frac{m+n\sqrt{D}}{2}\cdot\frac{m-n\sqrt{D}}{2} = \frac{m^2-Dn^2}{4} = \pm1$, we may introduce the Legendre symbol $\big(\frac{\varepsilon_D}{p}\big)$. When the norm $N(\varepsilon_D) = (m^2-Dn^2)/4 = -1$, many mathematicians tried to characterize those primes p for which ε_D is a quadratic residue $\pmod p$ (that is $\big(\frac{\varepsilon_D}{p}\big) = 1$). In 1908, Vandiver [V] found that $\varepsilon_5 = (1+\sqrt{5})/2$ is a quadratic residue of a prime $p\equiv 1,9 \pmod{20}$ if and only if $p = x^2+20y^2$ for some $x,y\in\mathbb{Z}$. In 1942 Aigner and Reichardt [AR] proved that $\varepsilon_2 = 1+\sqrt{2}$ is a quadratic residue of a prime $p\equiv 1 \pmod 8$ if and only if $p = x^2+32y^2 (x,y\in\mathbb{Z})$. In 1969, Barrucand and Cohn [BC] rediscovered this result. Later, Brandler [B] showed that for $q = 13, 37$ the unit ε_q is a quadratic residue of a prime p ($p\equiv 1 \pmod 4$, $(\frac{q}{p}) = 1$) if and only if $p = x^2+4qy^2 (x,y\in\mathbb{Z})$. For more special results along this line one may consult [BLW, LW1, LW2, Wi4], [Su6, Remark 6.1] and [Lem2, pp.168-180].

Let p and q be distinct primes such that $p\equiv q\equiv 1 \pmod 4$ and $\big(\frac{q}{p}\big) = \big(\frac{p}{q}\big) = 1$. Define

$$\Big[\frac{q}{p}\Big]_4 = \begin{cases} 1 & \text{if } q \text{ is a quartic residue } (\text{mod } p), \\ -1 & \text{if } q \text{ is a quartic nonresidue } (\text{mod } p). \end{cases}$$

According to [Lem2], in 1839 Schönemann [Sc] showed that

$$\Big(\frac{\varepsilon_p}{q}\Big) = \Big[\frac{q}{p}\Big]_4\Big[\frac{p}{q}\Big]_4 = \Big(\frac{\varepsilon_q}{p}\Big).$$

This was rediscovered by Scholz [S] in 1934, and it is now called Scholz's law. In [Su1] the author proved $\left(\frac{\varepsilon_p}{q}\right)=\left(\frac{\varepsilon_q}{p}\right)$ using only the quadratic reciprocity law. If $p=a^2+b^2$ and $q=c^2+d^2$ with $a,b,c,d\in\mathbb{Z}$ and $2\nmid ac$, in 1969 Burde [Bu] established the following Burde's rational quartic reciprocity law:

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

In 1985, Williams, Hardy and Friesen [WHF] found a general rational quartic reciprocity law including Scholz's law and Burde's law. See also [Lem1,Lem2] and [E1].

Let $D>1$ be a squarefree integer. There are a great many papers discussing $\left(\frac{\varepsilon_D}{p}\right)$. The problem of determining the value of $\left(\frac{\varepsilon_D}{p}\right)$ is concerned with quartic residues, rational quartic reciprocity laws, class numbers and binary quadratic forms, and many mathematicians discussed the problem by using class field theory. For more references, see for example, [Bro1, Bro2, D, FK, KWY, K, Le1-Le5, LW3, W, Wi1-Wi3, Wi5].

In [Su6], the author proved the following general result (see [Su6, Theorem 6.2 and Remark 6.1]).

Theorem 1.1. *Suppose that $p\equiv 1\pmod 4$ is a prime, $D,m,n\in\mathbb{Z}$, $m^2-Dn^2=-4$ and $\left(\frac{D}{p}\right)=1$. Then $(m+n\sqrt{D})/2$ is a quadratic residue $\pmod p$ if and only if p is represented by a primitive, integral quadratic form $ax^2+2bxy+cy^2$ of discriminant $-4k^2D$ with the condition that $2\nmid a$ and $\left(\frac{bn-kmi}{a}\right)_4=1$, where*

$$k=\begin{cases}1 & \text{if } D\equiv 4\pmod 8,\\ 2 & \text{if } 2\nmid D \text{ or } 8\mid D,\\ 4 & \text{if } D\equiv 2\pmod 4.\end{cases}$$

Let $p\equiv 1\pmod 4$ be a prime and $a,b\in\mathbb{Z}$ with $p\nmid a(a^2+b^2)$. If $s^2\equiv a^2+b^2\pmod p$ with $s\in\mathbb{Z}$, then clearly $(\frac{b+s}{p})(\frac{b-s}{p})=(\frac{b^2-s^2}{p})=(\frac{-a^2}{p})=1$. Thus we may define

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

In Section 2 we give general congruences for $\left(\frac{b+\sqrt{a^2+b^2}}{2}\right)^{\frac{p-1}{2}}\pmod p$ and deduce general criteria for $(\frac{\varepsilon_D}{p})=1$. For example, if $D>1$ is odd, $\varepsilon_D=(m+n\sqrt{D})/2$ and $N(\varepsilon_D)=-1$, and if $p=c^2+d^2$ with $c,d\in\mathbb{Z}$, $2\nmid c$, $p\nmid n$ and $\left(\frac{D}{p}\right)=1$, then

$$\left(\frac{\varepsilon_D}{p}\right)=\left(\frac{(m+\sqrt{m^2+2^2})/2}{p}\right)=\begin{cases}(\frac{mc+2d}{D}) & \text{if } 2\nmid m,\\ (\frac{c-\frac{m}{2}d}{D}) & \text{if } 2\mid m.\end{cases}$$

To our surprise, the result is very simple and it can be easily deduced from the law of quadratic reciprocity. If $4\nmid a^2+b^2$ and $(\frac{a^2+b^2}{p})=1$, in Section 4 we determine $\big(\frac{(b+\sqrt{a^2+b^2})/2}{p}\big)$ by expressing p in terms of binary quadratic forms of discriminant $-4(a^2+b^2)$. For example, if $p=x^2+(a^2+b^2)y^2$ for some integers x and y, we have

$$\Big(\frac{(b+\sqrt{a^2+b^2})/2}{p}\Big)=\begin{cases}(-1)^{\frac a2y} & \text{if } 2\mid a \text{ and } 2\nmid b,\\ (-1)^{\frac{p-1}4+\frac b2y} & \text{if } 2\nmid a \text{ and } 2\mid b,\\ (-1)^{\frac y2} & \text{if } 2\nmid ab.\end{cases}$$

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

(1.1) $U_0(b,a)=0,\ U_1(b,a)=1,\ U_{n+1}(b,a)=bU_n(b,a)-aU_{n-1}(b,a)\ (n\ge 1)$

and

(1.2) $V_0(b,a)=2,\ V_1(b,a)=b,\ V_{n+1}(b,a)=bV_n(b,a)-aV_{n-1}(b,a)\ (n\ge 1)$.

Let $\Delta=b^2-4a$. It is well known that

$$U_n(b,a)=\begin{cases}\frac{1}{\sqrt\Delta}\big\{\big(\frac{b+\sqrt\Delta}{2}\big)^n-\big(\frac{b-\sqrt\Delta}{2}\big)^n\big\} & \text{if } \Delta\ne 0,\\ n\big(\frac b2\big)^{n-1} & \text{if } \Delta=0\end{cases}\tag{1.3}$$

and

$$V_n(b,a)=\Big(\frac{b+\sqrt\Delta}{2}\Big)^n+\Big(\frac{b-\sqrt\Delta}{2}\Big)^n.\tag{1.4}$$

Suppose $p\equiv 1\pmod 4$ is a prime, $b,k\in\mathbb{Z}$ and $p\nmid k(b^2+4k^2)$. Using the results in Sections 2 and 4, in Sections 3 and 5 we determine $U_{\frac{p-1}2}(b,-k^2)$ and $V_{\frac{p-1}2}(b,-k^2)$ modulo p. As an application, we give general criteria for $p\mid U_{\frac{p-1}4}(b,-k^2)$.

In addition to the above notation, throughout this paper we let $\mathbb{N}$ denote the set of positive integers. For $a,b\in\mathbb{Z}$ (not both zero) let (a,b) be the greatest common divisor of a and b. For a given prime p and a nonzero integer n we use $\mathrm{ord}_p n$ to denote the nonnegative integer α such that $p^\alpha\mid n$ but $p^{\alpha+1}\nmid n$ (i.e. $p^\alpha\parallel n$).

2. Congruences for $\big(\frac{b+\sqrt{a^2+b^2}}{2}\big)^{\frac{p-1}2}\pmod p$ when $p=c^2+d^2$.

For two integers a and b, it is easily seen that (see [Su1])

$$(b+ai)\frac{b+\sqrt{a^2+b^2}}{2}=\Big(\frac{b+ai+\sqrt{a^2+b^2}}{2}\Big)^2.\tag{2.1}$$

This is the starting point for our goal.

Theorem 2.1. *Let $p \equiv 1 \pmod 4$ be a prime and $p = c^2 + d^2$ with $c, d \in \mathbb{Z}$ and $2 \nmid c$. Suppose $a, b \in \mathbb{Z}$ with $(a, b) = 1$ and $p \nmid a(a^2 + b^2)$.*

(i) *If $\left(\frac{a^2+b^2}{p}\right) = 1$, then*

$$\left(\frac{(b+\sqrt{a^2+b^2})/2}{p}\right) = \begin{cases} \left(\frac{bc+ad}{a^2+b^2}\right) & \text{if } 2 \mid a, \\ (-1)^{\frac{d}{2}}\left(\frac{ac-bd}{a^2+b^2}\right) & \text{if } 2 \mid b, \\ (-1)^{\frac{(bc+ad)^2-1}{8}}\left(\frac{bc+ad}{(a^2+b^2)/2}\right) & \text{if } 2 \nmid ab. \end{cases}$$

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

$$\begin{aligned} &\left(\frac{b+\sqrt{a^2+b^2}}{2}\right)^{\frac{p-1}{2}} \\ &\equiv \begin{cases} \left(\frac{bc+ad}{a^2+b^2}\right)\frac{c}{d} \cdot \frac{b-\sqrt{a^2+b^2}}{a} \pmod p & \text{if } 2 \mid a, \\ (-1)^{\frac{d}{2}}\left(\frac{ac-bd}{a^2+b^2}\right)\frac{c}{d} \cdot \frac{b-\sqrt{a^2+b^2}}{a} \pmod p & \text{if } 2 \mid b, \\ (-1)^{\frac{(bc+ad)^2-1}{8}}\left(\frac{bc+ad}{(a^2+b^2)/2}\right)\frac{c}{d} \cdot \frac{b-\sqrt{a^2+b^2}}{a} \pmod p & \text{if } 2 \nmid ab. \end{cases} \end{aligned}$$

Proof. We first evaluate the Legendre symbol $\left(\frac{b+ad/c}{p}\right)$. As $(b+ad/c)(b-ad/c) \equiv b^2 + a^2 \not\equiv 0 \pmod p$ we have $\left(\frac{b+ad/c}{p}\right) \neq 0$. It is known that $\left(\frac{c}{p}\right) = \left(\frac{p}{c}\right) = \left(\frac{c^2+d^2}{c}\right) = \left(\frac{d^2}{c}\right) = 1$ and $\left(\frac{d}{p}\right) = (-1)^{\frac{p-1}{4}} = (-1)^{\frac{d}{2}}$. Thus,

$$\left(\frac{b+ad/c}{p}\right) = \left(\frac{bc+ad}{p}\right) = \left(\frac{d}{p}\right)\left(\frac{a-bd/c}{p}\right) = (-1)^{\frac{d}{2}}\left(\frac{ac-bd}{p}\right).$$

Now we assert that $(a^2+b^2, bc+ad) = (a^2+b^2, ac-bd) = 1$. If q is a prime such that $q \mid (a^2+b^2, bc+ad)$, we have $-a^2c^2 \equiv b^2c^2 \equiv a^2d^2 \pmod q$ and so $q \mid a^2p$. As $p \nmid a^2+b^2$ and $q \mid a^2+b^2$ we see that $q \neq p$. Thus $q \mid a$ and so $q \mid b$. This contradicts the condition $(a, b) = 1$. Hence $(a^2+b^2, bc+ad) = 1$. Similarly we have $(a^2+b^2, ac-bd) = 1$. So the assertion is true.

If $2 \mid a$, then $2 \nmid b$. By the above we have $(a^2+b^2, bc+ad) = 1$ and so

$$\begin{aligned} \left(\frac{b+ad/c}{p}\right) &= \left(\frac{bc+ad}{p}\right) = \left(\frac{p}{bc+ad}\right) = \left(\frac{(a^2+b^2)(c^2+d^2)}{bc+ad}\right)\left(\frac{a^2+b^2}{bc+ad}\right) \\ &= \left(\frac{(bc+ad)^2+(ac-bd)^2}{bc+ad}\right)\left(\frac{bc+ad}{a^2+b^2}\right) \\ &= \left(\frac{(ac-bd)^2}{bc+ad}\right)\left(\frac{bc+ad}{a^2+b^2}\right) = \left(\frac{bc+ad}{a^2+b^2}\right). \end{aligned}$$

If $2 \mid b$, then $2 \nmid a$. From the above we have $(a^2+b^2, ac-bd) = 1$ and so

$$\begin{aligned}\Big(\frac{b+ad/c}{p}\Big) &= (-1)^{\frac{d}{2}}\Big(\frac{ac-bd}{p}\Big) = (-1)^{\frac{d}{2}}\Big(\frac{p}{ac-bd}\Big)\\ &= (-1)^{\frac{d}{2}}\Big(\frac{(a^2+b^2)(c^2+d^2)}{ac-bd}\Big)\Big(\frac{a^2+b^2}{ac-bd}\Big)\\ &= (-1)^{\frac{d}{2}}\Big(\frac{(ac-bd)^2+(bc+ad)^2}{ac-bd}\Big)\Big(\frac{ac-bd}{a^2+b^2}\Big)\\ &= (-1)^{\frac{d}{2}}\Big(\frac{ac-bd}{a^2+b^2}\Big).\end{aligned}$$

If $2 \nmid ab$, then $(a^2+b^2)/2 \equiv 1 \pmod 4$. By the previous assertion we have $(a^2+b^2, bc+ad) = 1$ and so $((a^2+b^2)/2, bc+ad) = 1$. Hence

$$\begin{aligned}\Big(\frac{b+ad/c}{p}\Big) &= \Big(\frac{bc+ad}{p}\Big) = \Big(\frac{p}{bc+ad}\Big)\\ &= \Big(\frac{2}{bc+ad}\Big)\Big(\frac{(c^2+d^2)(a^2+b^2)}{bc+ad}\Big)\Big(\frac{(a^2+b^2)/2}{bc+ad}\Big)\\ &= \Big(\frac{2}{bc+ad}\Big)\Big(\frac{(bc+ad)^2+(ac-bd)^2}{bc+ad}\Big)\Big(\frac{bc+ad}{(a^2+b^2)/2}\Big)\\ &= \Big(\frac{2}{bc+ad}\Big)\Big(\frac{bc+ad}{(a^2+b^2)/2}\Big) = (-1)^{\frac{(bc+ad)^2-1}{8}}\Big(\frac{bc+ad}{(a^2+b^2)/2}\Big).\end{aligned}$$

Note that $(d/c)^2 \equiv -1 \pmod p$. From (2.1) we have

$$(2.2)\quad (b+ad/c)^{\frac{p-1}{2}}\Big(\frac{b+\sqrt{a^2+b^2}}{2}\Big)^{\frac{p-1}{2}} \equiv (b+ad/c+\sqrt{a^2+b^2})^{p-1} \pmod p.$$

As $p \nmid a(a^2+b^2)$ we see that $b+ad/c \not\equiv 0 \pmod p$, $b+\sqrt{a^2+b^2} \not\equiv 0 \pmod p$ and so $b+ad/c+\sqrt{a^2+b^2} \not\equiv 0 \pmod p$.

Now we assume $(\frac{a^2+b^2}{p}) = 1$. By the above we have

$$\Big(\frac{(b+\sqrt{a^2+b^2})/2}{p}\Big)\Big(\frac{b+ad/c}{p}\Big) = \Big(\frac{b+ad/c+\sqrt{a^2+b^2}}{p}\Big)^2 = 1.$$

Thus

$$\Big(\frac{(b+\sqrt{a^2+b^2})/2}{p}\Big) = \Big(\frac{b+ad/c}{p}\Big).$$

This together with the previous evaluation of $(\frac{b+ad/c}{p})$ proves (i).

Let us consider (ii). Suppose $(\frac{a^2+b^2}{p}) = -1$. As

$$(\sqrt{a^2+b^2})^p = \sqrt{a^2+b^2}(a^2+b^2)^{\frac{p-1}{2}} \equiv -\sqrt{a^2+b^2} \pmod p,$$

we see that

$$\begin{aligned}(b+ad/c+\sqrt{a^2+b^2})^p &\equiv (b+ad/c)^p+(\sqrt{a^2+b^2})^p \\ &\equiv b+ad/c-\sqrt{a^2+b^2} \pmod p.\end{aligned}$$

Thus

$$\begin{aligned}(b+ad/c+\sqrt{a^2+b^2})^{p-1} &\equiv \frac{b+ad/c-\sqrt{a^2+b^2}}{b+ad/c+\sqrt{a^2+b^2}} \\ &\equiv \frac{(b-\sqrt{a^2+b^2})c}{ad} \pmod p.\end{aligned}$$

Combining this with (2.2) we obtain

$$\Big(\frac{b+\sqrt{a^2+b^2}}{2}\Big)^{\frac{p-1}{2}} \equiv \Big(\frac{b+ad/c}{p}\Big)\frac{(b-\sqrt{a^2+b^2})c}{ad} \pmod p.$$

Now applying the evaluation of $(\frac{b+ad/c}{p})$ we obtain (ii) and hence the theorem is proved.
Remark 2.1 When $2 \mid a$ and a^2+b^2 is a prime, Theorem 2.1(i) was known to E. Lehmer [Le2].

Lemma 2.1. *Let $D,m,n \in \mathbb{Z}$ with $m^2-Dn^2=-4$ and $2 \mid m$. Then*

$$m \equiv \begin{cases} 0 \pmod 4 & \text{if } 2 \nmid D \text{ or } 8 \mid D-4, \\ 2 \pmod 4 & \text{if } 4 \mid D-2 \text{ or } 8 \mid D. \end{cases}$$

Proof. As $(\frac{m}{2})^2-\frac{Dn^2}{4}=-1$ we see that $4 \mid Dn^2$ and $16 \nmid Dn^2$. If $4 \mid D$, then $2 \nmid n$. Thus $m/2 \equiv (m/2)^2 = n^2D/4-1 \equiv D/4-1 \pmod 2$ and so $m \equiv D/2-2 \pmod 4$. If $4 \mid D-2$, then $2 \mid n$ and so $(\frac{m}{2})^2 = D(\frac{n}{2})^2-1 \equiv 1 \pmod 2$ and so $4 \mid m-2$. If $2 \nmid D$, then $4 \mid n^2$ and $16 \nmid n^2$. Thus $n \equiv 2 \pmod 4$. Hence $(\frac{m}{2})^2 = D(\frac{n}{2})^2-1 \equiv 0 \pmod 2$ and so $4 \mid m$. Now the proof is complete.

Theorem 2.2. *Let $D,m,n \in \mathbb{Z}$ with $m^2-Dn^2=-4$. Let $p \equiv 1 \pmod 4$ be a prime such that $p \nmid Dn$. Let $p=c^2+d^2 (c,d \in \mathbb{Z})$ with $2 \nmid c$ and let*

$$\delta = \begin{cases} \big(\frac{mc+2d}{D}\big) & \text{if } 2 \nmid m, \\ (-1)^{\frac{(\frac{m}{2}c+d)^2-1}{8}+\frac{d}{2}}\big(\frac{\frac{m}{2}c+d}{D/2}\big) & \text{if } 4 \mid D-2, \\ (-1)^{\frac{(\frac{m}{2}c+d)^2-1}{8}+\frac{d}{2}}\big(\frac{\frac{m}{2}c+d}{D/8}\big) & \text{if } 8 \mid D, \\ \big(\frac{c-\frac{m}{2}d}{D}\big) & \text{if } 2 \nmid D \text{ and } 2 \mid m, \\ \big(\frac{c-\frac{m}{2}d}{D/4}\big) & \text{if } 8 \mid D-4. \end{cases}$$

Then

$$\Big(\frac{m+n\sqrt{D}}{2}\Big)^{\frac{p-1}{2}} \equiv \begin{cases} \delta \pmod p & \text{if } (\frac{D}{p})=1, \\ \delta\frac{c}{d}\cdot\frac{m-n\sqrt{D}}{2} \pmod p & \text{if } (\frac{D}{p})=-1. \end{cases}$$

Proof. We first assume $(\frac{D}{p})=1$. As $m^2-Dn^2=-4$ we have $\big(\frac{(m+n\sqrt{D})/2}{p}\big) \neq 0$. If $2\nmid m$, then clearly $2\nmid Dn$. Taking $a=2$ and $b=m$ in Theorem 2.1(i) we see that

$$\begin{aligned}\Big(\frac{(m+n\sqrt{D})/2}{p}\Big) &= \Big(\frac{(m+\sqrt{2^2+m^2})/2}{p}\Big) = \Big(\frac{mc+2d}{2^2+m^2}\Big) \\ &= \Big(\frac{mc+2d}{Dn^2}\Big) = \Big(\frac{mc+2d}{D}\Big).\end{aligned}$$

So the result is true. If $4\mid D-2$ or $8\mid D$, then clearly $2\mid m$. By Lemma 2.1 we have $m\equiv 2 \pmod 4$ and so $\frac{Dn^2}{8}=\frac{m^2+4}{8}\equiv 1 \pmod 2$. Thus applying Theorem 2.1(i) and the fact $(\frac{2}{p})=(-1)^{\frac{p-1}{4}}=(-1)^{\frac{d}{2}}$ we see that

$$\begin{aligned}\Big(\frac{(m+n\sqrt{D})/2}{p}\Big) &= \Big(\frac{\frac{m}{2}+\sqrt{(\frac{m}{2})^2+1}}{p}\Big) = \Big(\frac{2}{p}\Big)(-1)^{\frac{(\frac{m}{2}c+d)^2-1}{8}}\Big(\frac{\frac{m}{2}c+d}{(m^2+4)/8}\Big) \\ &= (-1)^{\frac{(\frac{m}{2}c+d)^2-1}{8}+\frac{d}{2}}\Big(\frac{\frac{m}{2}c+d}{Dn^2/8}\Big) = \delta.\end{aligned}$$

If $2\nmid D$ and $2\mid m$ or if $8\mid D-4$, by Lemma 2.1 we have $4\mid m$ and so $\frac{Dn^2}{4}=(\frac{m}{2})^2+1\equiv 1 \pmod 2$. Thus applying Theorem 2.1(i) we have

$$\begin{aligned}\Big(\frac{(m+n\sqrt{D})/2}{p}\Big) &= \Big(\frac{\frac{m}{2}+\sqrt{(\frac{m}{2})^2+1}}{p}\Big) = \Big(\frac{2}{p}\Big)(-1)^{\frac{d}{2}}\Big(\frac{c-\frac{m}{2}d}{(\frac{m}{2})^2+1}\Big) \\ &= \Big(\frac{c-\frac{m}{2}d}{Dn^2/4}\Big) = \delta.\end{aligned}$$

When $(\frac{D}{p})=-1$, one can similarly prove the result by using Theorem 2.1(ii). Thus the theorem is proved.

As consequences of Theorem 2.2 we have:

Corollary 2.1. *Suppose that* $p\equiv 1 \pmod 4$ *is a prime and* $p=c^2+d^2 (c,d\in\mathbb{Z})$ *with* $2\mid d$. *Then*

$$(1+\sqrt{2})^{\frac{p-1}{2}} \equiv \begin{cases} (-1)^{\frac{(c+d)^2-1}{8}} \pmod p & \text{if } p\equiv 1 \pmod 8, \\ -(-1)^{\frac{(c+d)^2-1}{8}}\frac{c}{d}(1-\sqrt{2}) \pmod p & \text{if } p\equiv 5 \pmod 8) \end{cases}$$

and

$$\Big(\frac{1+\sqrt5}{2}\Big)^{\frac{p-1}{2}}\equiv\begin{cases}\big(\frac{c+2d}{5}\big)\pmod p & \text{if } p\equiv 1,9 \pmod{20},\\ \big(\frac{c+2d}{5}\big)\frac cd\cdot\frac{1-\sqrt5}{2}\pmod p & \text{if } p\equiv 13,17\pmod{20}.\end{cases}$$

Proof. Taking $m=n=2$ and $D=2$ in Theorem 2.2 we obtain the congruence for $(1+\sqrt2)^{\frac{p-1}{2}} \pmod p$. Taking $m=n=1$ and $D=5$ in Theorem 2.2 we obtain the remaining result.

Remark 2.2 When $p\equiv 1 \pmod 8$ is a prime and $p=c^2+d^2$ with $2\mid d$, the congruence $(1+\sqrt2)^{\frac{p-1}{2}}\equiv(-1)^{\frac{p-1}{8}+\frac d4}\pmod p$ was observed by Lehmer in [Le4].

Using Theorem 2.2 one can also deduce the following results.

Corollary 2.2. *Suppose that* $p\equiv 1\pmod 4$ *is a prime and* $p=c^2+d^2 (c,d\in\mathbb Z)$ *with* $2\mid d$. *Then*

$$\begin{aligned}&(3+\sqrt{10})^{\frac{p-1}{2}}\\ &\equiv\begin{cases}(-1)^{\frac{(3c+d)^2-1}{8}+\frac d2}\big(\frac{3c+d}{5}\big)\pmod p & \text{if } p\equiv 1,9,13,37\pmod{40},\\ (-1)^{\frac{(3c+d)^2-1}{8}+\frac d2}\big(\frac{3c+d}{5}\big)\frac cd(3-\sqrt{10})\pmod p & \text{if } p\equiv 17,21,29,33\pmod{40}\end{cases}\end{aligned}$$

and

$$\Big(\frac{3+\sqrt{13}}{2}\Big)^{\frac{p-1}{2}}\equiv\begin{cases}\big(\frac{3c+2d}{13}\big)\pmod p & \text{if } p\equiv\pm1,\pm3,\pm4\pmod{13},\\ \big(\frac{3c+2d}{13}\big)\frac cd\cdot\frac{3-\sqrt{13}}{2}\pmod p & \text{if } p\equiv\pm2,\pm5,\pm6\pmod{13}.\end{cases}$$

Corollary 2.3. *Suppose that* $p\equiv 1\pmod 4$ *is a prime and* $p=c^2+d^2 (c,d\in\mathbb Z)$ *with* $2\mid d$. *Then*

$$\begin{aligned}&(4+\sqrt{17})^{\frac{p-1}{2}}\\ &\equiv\begin{cases}\big(\frac{c-4d}{17}\big)\pmod p & \text{if } p\equiv\pm1,\pm2,\pm4,\pm8\pmod{17},\\ \big(\frac{c-4d}{17}\big)\frac cd(4-\sqrt{17})\pmod p & \text{if } p\equiv\pm3,\pm5,\pm6,\pm7\pmod{17}\end{cases}\end{aligned}$$

and

$$\begin{aligned}&(5+\sqrt{26})^{\frac{p-1}{2}}\\ &\equiv\begin{cases}(-1)^{\frac{(5c+d)^2-1}{8}+\frac d2}\big(\frac{5c+d}{13}\big)\pmod p & \text{if } \big(\frac p{13}\big)=(-1)^{\frac{p-1}{4}},\\ (-1)^{\frac{(5c+d)^2-1}{8}+\frac d2}\big(\frac{5c+d}{13}\big)\frac cd(5-\sqrt{26})\pmod p & \text{if } \big(\frac p{13}\big)=-(-1)^{\frac{p-1}{4}}.\end{cases}\end{aligned}$$

Corollary 2.4. *Suppose that $p \equiv 1 \pmod 4$ is a prime and $p = c^2+d^2 (c,d \in \mathbb{Z})$ with $2 \mid d$. Then*

$$\Big(\frac{5+\sqrt{29}}{2}\Big)^{\frac{p-1}{2}} \equiv \begin{cases} (\frac{5c+2d}{29}) \pmod p & \text{if } (\frac{p}{29}) = 1, \\ (\frac{5c+2d}{29})\frac{c}{d}\cdot\frac{5-\sqrt{29}}{2} \pmod p & \text{if } (\frac{p}{29}) = -1 \end{cases}$$

and

$$(6+\sqrt{37})^{\frac{p-1}{2}} \equiv \begin{cases} (\frac{c-6d}{37}) \pmod p & \text{if } (\frac{p}{37}) = 1, \\ (\frac{c-6d}{37})\frac{c}{d}(6-\sqrt{37}) \pmod p & \text{if } (\frac{p}{37}) = -1. \end{cases}$$

3. Congruences for $U_{\frac{p\pm1}{2}}(b,-k^2) \pmod p$ when $p = c^2+d^2$.

For $a,b \in \mathbb{Z}$ let $\{U_n(b,a)\}$ and $\{V_n(b,a)\}$ be the Lucas sequences defined by (1.1) and (1.2). In the section we determine the values of $U_{\frac{p-1}{2}}(b,-k^2)$ and $V_{\frac{p-1}{2}}(b,-k^2) \pmod p$ and give criteria for $p \mid U_{\frac{p-1}{4}}(b,-k^2)$, where $b,k \in \mathbb{Z}$ and p is a prime such that $p = c^2+d^2 \equiv 1 \pmod 4$.

Theorem 3.1. *Let $p \equiv 1 \pmod 4$ be a prime and $p = c^2+d^2$ with $c,d \in \mathbb{Z}$ and $2 \mid d$. Let $b,k \in \mathbb{Z}$ with $(k,b) = 1$ and $p \nmid k(b^2+4k^2)$. Let*

$$I = \begin{cases} \Big(\frac{bc+2kd}{b^2+4k^2}\Big) & \text{if } 2 \nmid b, \\ (-1)^{\frac{(\frac{b}{2}c+kd)^2-1}{8}+\frac{d}{2}}\Big(\frac{\frac{b}{2}c+kd}{((\frac{b}{2})^2+k^2)/2}\Big) & \text{if } 2 \parallel b, \\ \Big(\frac{kc-\frac{b}{2}d}{(\frac{b}{2})^2+k^2}\Big) & \text{if } 4 \mid b. \end{cases}$$

Then

$$U_{\frac{p-1}{2}}(b,-k^2) \equiv \begin{cases} 0 \pmod p & \text{if } (\frac{b^2+4k^2}{p}) = 1, \\ -\frac{c}{kd}I \pmod p & \text{if } (\frac{b^2+4k^2}{p}) = -1 \end{cases}$$

and

$$V_{\frac{p-1}{2}}(b,-k^2) \equiv \begin{cases} 2I \pmod p & \text{if } (\frac{b^2+4k^2}{p}) = 1, \\ \frac{bc}{kd}I \pmod p & \text{if } (\frac{b^2+4k^2}{p}) = -1. \end{cases}$$

Proof. If $2 \nmid b$, taking $a = 2k$ in Theorem 2.1 we see that

$$\Big(\frac{b\pm\sqrt{b^2+4k^2}}{2}\Big)^{\frac{p-1}{2}} \equiv \begin{cases} (\frac{bc+2kd}{b^2+4k^2}) \pmod p & \text{if } (\frac{b^2+4k^2}{p}) = 1, \\ (\frac{bc+2kd}{b^2+4k^2})\frac{c}{d}\cdot\frac{b\mp\sqrt{b^2+4k^2}}{2k} \pmod p & \text{if } (\frac{b^2+4k^2}{p}) = -1. \end{cases}$$

Thus

$$U_{\frac{p-1}{2}}(b,-k^2)=\frac{1}{\sqrt{b^2+4k^2}}\Big\{\Big(\frac{b+\sqrt{b^2+4k^2}}{2}\Big)^{\frac{p-1}{2}}-\Big(\frac{b-\sqrt{b^2+4k^2}}{2}\Big)^{\frac{p-1}{2}}\Big\}$$
$$\equiv\begin{cases}0 \pmod p & \text{if } (\frac{b^2+4k^2}{p})=1,\\ -\frac{c}{kd}(\frac{bc+2kd}{b^2+4k^2}) \pmod p & \text{if } (\frac{b^2+4k^2}{p})=-1\end{cases}$$

and

$$V_{\frac{p-1}{2}}(b,-k^2)=\Big(\frac{b+\sqrt{b^2+4k^2}}{2}\Big)^{\frac{p-1}{2}}+\Big(\frac{b-\sqrt{b^2+4k^2}}{2}\Big)^{\frac{p-1}{2}}$$
$$\equiv\begin{cases}2(\frac{bc+2kd}{b^2+4k^2}) \pmod p & \text{if } (\frac{b^2+4k^2}{p})=1,\\ \frac{bc}{kd}(\frac{bc+2kd}{b^2+4k^2}) \pmod p & \text{if } (\frac{b^2+4k^2}{p})=-1.\end{cases}$$

If $2\parallel b$, then $2\nmid k$. By Theorem 2.1 and the fact $\big(\frac{2}{p}\big)=(-1)^{\frac d2}$ we have

$$\Big(\frac{b\pm\sqrt{b^2+4k^2}}{2}\Big)^{\frac{p-1}{2}}$$
$$\equiv\Big(\frac{2}{p}\Big)\Big(\frac{\frac b2\pm\sqrt{(\frac b2)^2+k^2}}{2}\Big)^{\frac{p-1}{2}}$$
$$\equiv\begin{cases}(-1)^{\frac{(\frac b2c+kd)^2-1}{8}+\frac d2}\big(\frac{\frac b2c+kd}{((\frac b2)^2+k^2)/2}\big) \pmod p & \text{if } (\frac{b^2+4k^2}{p})=1,\\ (-1)^{\frac{(\frac b2c+kd)^2-1}{8}+\frac d2}\big(\frac{\frac b2c+kd}{((\frac b2)^2+k^2)/2}\big)\frac cd\cdot\frac{\frac b2\mp\sqrt{(\frac b2)^2+k^2}}{k} \pmod p & \\ \qquad\qquad\qquad\qquad \text{if } (\frac{b^2+4k^2}{p})=-1.\end{cases}$$

This together with (1.3) and (1.4) yields the result in this case.

If $4\mid b$, using Theorem 2.1 we see that

$$\Big(\frac{b\pm\sqrt{b^2+4k^2}}{2}\Big)^{\frac{p-1}{2}}$$
$$\equiv\Big(\frac{2}{p}\Big)\Big(\frac{\frac b2\pm\sqrt{(\frac b2)^2+k^2}}{2}\Big)^{\frac{p-1}{2}}$$
$$\equiv\begin{cases}\big(\frac{kc-\frac b2d}{(\frac b2)^2+k^2}\big) \pmod p & \text{if } (\frac{b^2+4k^2}{p})=1,\\ \big(\frac{kc-\frac b2d}{(\frac b2)^2+k^2}\big)\frac cd\cdot\frac{\frac b2\mp\sqrt{(\frac b2)^2+k^2}}{k} \pmod p & \text{if } (\frac{b^2+4k^2}{p})=-1.\end{cases}$$

Now applying (1.3) and (1.4) we deduce the result. The proof is now complete.

Remark 3.1 Let $a,b\in\mathbb{Z}$ and p be an odd prime such that $(\frac ap)=1$ and $p\nmid b^2-4a$. It is well known that $p\mid U_{(p-(\frac{b^2-4a}{p}))/2}(b,a)$, see [L]. Thus, if $p\equiv 1\pmod 4$, $p\nmid k$ and $(\frac{b^2+4k^2}{p})=1$, then $p\mid U_{\frac{p-1}{2}}(b,-k^2)$.

Putting $b=1,2,3,8$ and $k=1$ in Theorem 3.1 we deduce the following results.

Corollary 3.1. *Let $p \equiv 1 \pmod 4$ be a prime and $p = c^2 + d^2$ with $c, d \in \mathbb{Z}$ and $2 \mid d$. Let $F_n = U_n(1,-1)$ and $L_n = V_n(1,-1)$ be the Fibonacci and Lucas sequences respectively. Then*

$$F_{\frac{p-1}{2}} \equiv \begin{cases} 0 \pmod p & \text{if } p \equiv 1, 9 \pmod{20}, \\ -(\frac{c+2d}{5})\frac{c}{d} \pmod p & \text{if } p \equiv 13, 17 \pmod{20} \end{cases}$$

and

$$L_{\frac{p-1}{2}} \equiv \begin{cases} 2(\frac{c+2d}{5}) \pmod p & \text{if } p \equiv 1, 9 \pmod{20}, \\ (\frac{c+2d}{5})\frac{c}{d} \pmod p & \text{if } p \equiv 13, 17 \pmod{20}. \end{cases}$$

Corollary 3.2. *Let $p \equiv 1 \pmod 4$ be a prime and $p = c^2 + d^2$ with $c, d \in \mathbb{Z}$ and $2 \mid d$. Then*

$$U_{\frac{p-1}{2}}(2,-1) \equiv \begin{cases} 0 \pmod p & \text{if } p \equiv 1 \pmod 8, \\ (-1)^{\frac{(c+d)^2-1}{8}}\frac{c}{d} \pmod p & \text{if } p \equiv 5 \pmod 8 \end{cases}$$

and

$$V_{\frac{p-1}{2}}(2,-1) \equiv \begin{cases} 2(-1)^{\frac{(c+d)^2-1}{8}} \pmod p & \text{if } p \equiv 1 \pmod 8, \\ -2(-1)^{\frac{(c+d)^2-1}{8}}\frac{c}{d} \pmod p & \text{if } p \equiv 5 \pmod 8. \end{cases}$$

Corollary 3.3. *Let $p \equiv 1 \pmod 4$ be a prime and $p = c^2 + d^2$ with $c, d \in \mathbb{Z}$ and $2 \mid d$. Then*

$$U_{\frac{p-1}{2}}(3,-1) \equiv \begin{cases} 0 \pmod p & \text{if } p \equiv \pm1, \pm3, \pm4 \pmod{13}, \\ -(\frac{3c+2d}{13})\frac{c}{d} \pmod p & \text{if } p \equiv \pm2, \pm5, \pm6 \pmod{13} \end{cases}$$

and

$$V_{\frac{p-1}{2}}(3,-1) \equiv \begin{cases} 2(\frac{3c+2d}{13}) \pmod p & \text{if } p \equiv \pm1, \pm3, \pm4 \pmod{13}, \\ 3(\frac{3c+2d}{13})\frac{c}{d} \pmod p & \text{if } p \equiv \pm2, \pm5, \pm6 \pmod{13}. \end{cases}$$

Corollary 3.4. *Let $p \equiv 1 \pmod 4$ be a prime and $p = c^2 + d^2$ with $c, d \in \mathbb{Z}$ and $2 \mid d$. Then*

$$U_{\frac{p-1}{2}}(8,-1) \equiv \begin{cases} 0 \pmod p & \text{if } p \equiv \pm1, \pm2, \pm4, \pm8 \pmod{17}, \\ -(\frac{c-4d}{17})\frac{c}{d} \pmod p & \text{if } p \equiv \pm3, \pm5, \pm6, \pm7 \pmod{17} \end{cases}$$

and

$$V_{\frac{p-1}{2}}(8,-1) \equiv \begin{cases} 2(\frac{c-4d}{17}) \pmod p & \text{if } p \equiv \pm1, \pm2, \pm4, \pm8 \pmod{17}, \\ (\frac{c-4d}{17})\frac{8c}{d} \pmod p & \text{if } p \equiv \pm3, \pm5, \pm6, \pm7 \pmod{17}. \end{cases}$$

Theorem 3.2. *Let $p \equiv 1 \pmod 4$ be a prime and $p = c^2 + d^2$ with $c, d \in \mathbb{Z}$ and $2 \mid d$. Let $b, k \in \mathbb{Z}$ with $(k, b) = 1$ and $p \nmid k(b^2 + 4k^2)$. Let I be as in Theorem 3.1. Then*

$$U_{\frac{p+1}{2}}(b, -k^2) \equiv \begin{cases} I \pmod p & \text{if } (\frac{b^2+4k^2}{p}) = 1, \\ 0 \pmod p & \text{if } (\frac{b^2+4k^2}{p}) = -1 \end{cases}$$

and

$$V_{\frac{p+1}{2}}(b, -k^2) \equiv \begin{cases} bI \pmod p & \text{if } (\frac{b^2+4k^2}{p}) = 1, \\ -\frac{2kc}{d} I \pmod p & \text{if } (\frac{b^2+4k^2}{p}) = -1. \end{cases}$$

Proof. Let $U_n = U_n(b, -k^2)$ and $V_n = V_n(b, -k^2)$. From (1.3) and (1.4) we see that

$$(3.1) \quad U_{\frac{p+1}{2}} = \frac{1}{2}\big(bU_{\frac{p-1}{2}} + V_{\frac{p-1}{2}}\big) \text{ and } V_{\frac{p+1}{2}} = \frac{1}{2}\big((b^2+4k^2)U_{\frac{p-1}{2}} + bV_{\frac{p-1}{2}}\big).$$

Thus applying Theorem 3.1 we obtain the result.

Theorem 3.3. *Let $p \equiv 1 \pmod 4$ be a prime and $p = c^2 + d^2$ with $c, d \in \mathbb{Z}$ and $2 \mid d$. Let $b, k \in \mathbb{Z}$ with $(k, b) = 1$, $p \nmid k$ and $\big(\frac{b^2+4k^2}{p}\big) = 1$. Let I be as in Theorem 3.1. Then $p \mid U_{\frac{p-1}{4}}(b, -k^2)$ if and only if $I = \big(\frac{2k}{p}\big)$.*

Proof. Set $U_n = U_n(b, -k^2)$ and $V_n = V_n(b, -k^2)$. From [Su3, Lemma 6.1] we know that

$$(3.2) \qquad p \mid U_{\frac{p-1}{4}} \iff V_{\frac{p-1}{2}} \equiv 2(-k^2)^{\frac{p-1}{4}} \equiv 2\Big(\frac{2k}{p}\Big) \pmod p.$$

Thus applying Theorem 3.1 we have

$$\begin{aligned} p \mid U_{\frac{p-1}{4}} &\iff V_{\frac{p-1}{2}} \equiv 2\Big(\frac{2k}{p}\Big) \pmod p \iff 2I \equiv 2\Big(\frac{2k}{p}\Big) \pmod p \\ &\iff I = \Big(\frac{2k}{p}\Big). \end{aligned}$$

This proves the theorem.

Remark 3.2 Let $p \equiv 1 \pmod 4$ be a prime and $p = c^2 + d^2$ with $c, d \in \mathbb{Z}$ and $2 \mid d$. Let $b, k \in \mathbb{Z}$ with $(k, b) = 1$, $p \nmid k$ and $\big(\frac{b^2+4k^2}{p}\big) = -1$. By Theorem 3.1 we have $V_{\frac{p-1}{2}}(b, -k^2) \equiv \frac{bc}{kd} I \pmod p$. As $p \nmid k(b^2 + 4k^2)$ we see that $\frac{bc}{kd} \not\equiv \pm 2 \pmod p$ and so $V_{\frac{p-1}{2}}(b, -k^2) \not\equiv 2(\frac{2k}{p}) \pmod p$. Thus, by (3.2) we have $p \nmid U_{\frac{p-1}{4}}(b, -k^2)$.

From (1.3) and (1.4) we know that

$$U_n(bc, ac^2) = c^{n-1}U_n(b, a) \quad \text{and} \quad V_n(bc, ac^2) = c^n V_n(b, a).$$

Thus $U_n(b, -k^2) = (k, b)^{n-1}U_n(b', -k'^2)$ and $V_n(b, -k^2) = (k, b)^n V_n(b', -k'^2)$, where $k' = k/(k, b)$ and $b' = b/(k, b)$. Using this we may extend Theorems 3.1-3.3 to the case $(k, b) > 1$.

Putting $k = 1$ in Theorem 3.3 we obtain the following result.

Corollary 3.5. *Let $p\equiv 1 \pmod 4$ be a prime and $p=c^2+d^2$ with $c,d\in\mathbb{Z}$ and $2\mid d$. Let $b\in\mathbb{Z}$ and $\left(\frac{b^2+4}{p}\right)=1$. Let $\{U_n\}$ be given by $U_0=0,\ U_1=1$ and $U_{n+1}=bU_n+U_{n-1}(n\ge 1)$. Then*

$$p\mid U_{\frac{p-1}{4}} \iff \begin{cases} \left(\frac{bc+2d}{b^2+4}\right)=(-1)^{\frac d2} & \text{if } 2\nmid b,\\ \left(\frac{\frac b2 c+d}{(b^2+4)/8}\right)=(-1)^{\frac{(\frac b2 c+d)^2-1}{8}} & \text{if } 2\parallel b,\\ \left(\frac{c-\frac b2 d}{1+b^2/4}\right)=(-1)^{\frac d2} & \text{if } 4\mid b.\end{cases}$$

Remark 3.3 Let $p\equiv 1,9 \pmod{20}$ be a prime and $p=c^2+d^2$ with $c,d\in\mathbb{Z}$ and $2\mid d$. Then clearly $5\mid c$ or $5\mid d$. Let $F_n=U_n(1,-1)$ be the Fibonacci sequence. From Corollary 3.5 we deduce

$$p\mid F_{\frac{p-1}{4}} \iff \begin{cases} 5\mid c & \text{if } p\equiv 9,21 \pmod{40},\\ 5\mid d & \text{if } p\equiv 1,29 \pmod{40}.\end{cases}$$

This result is due to E. Lehmer [Le1].

4. Congruences for $\left(\frac{b+\sqrt{a^2+b^2}}{2}\right)^{\frac{p-1}{2}} \pmod p$ when $p=Ax^2+2Bxy+Cy^2$ and $AC-B^2=a^2+b^2$.

Lemma 4.1 ([E2], [Su1, Proposition 1], [Su4, 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*

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

Theorem 4.1. *Let p be an odd prime and $a,b\in\mathbb{Z}$ with $p\nmid a(a^2+b^2)$. Then*

$$\left(\frac{b+\sqrt{a^2+b^2}}{2\sqrt{a^2+b^2}}\right)^{\frac{p-1}{2}} \equiv \begin{cases} \pm 1 \pmod p & \text{if } \left(\frac{b+ai}{p}\right)_4=\pm 1,\\ \pm\frac{b-\sqrt{a^2+b^2}}{a} \pmod p & \text{if } \left(\frac{b+ai}{p}\right)_4=\pm i.\end{cases}$$

Proof. Substituting a,b,c by $-a^2,2b,-a$ in [Su5, Theorem 3.1 and Corollary 3.1] we see that

$$U_{\frac{p-1}{2}}(2b,-a^2)$$
$$\equiv \begin{cases} 0 \pmod p & \text{if } 4\mid p-1 \text{ and } \left(\frac{a^2+b^2}{p}\right)=1,\\ \frac1a(4a^2+4b^2)^{\frac{p-1}{4}}\left(\frac{2b+2ai}{p}\right)_4 i \pmod p & \text{if } 4\mid p-1 \text{ and } \left(\frac{a^2+b^2}{p}\right)=-1,\\ 2(4a^2+4b^2)^{\frac{p-3}{4}}\left(\frac{2b+2ai}{p}\right)_4 \pmod p & \text{if } 4\mid p-3 \text{ and } \left(\frac{a^2+b^2}{p}\right)=1,\\ -\frac{2b}{a}(4a^2+4b^2)^{\frac{p-3}{4}}\left(\frac{2b+2ai}{p}\right)_4 i \pmod p & \text{if } 4\mid p-3 \text{ and } \left(\frac{a^2+b^2}{p}\right)=-1\end{cases}$$

and

$$
\begin{aligned}
&V_{\frac{p-1}{2}}(2b,-a^2)\\
&\equiv \begin{cases} 2(4a^2+4b^2)^{\frac{p-1}{4}}\left(\frac{2b+2ai}{p}\right)_4 \pmod p & \text{if } 4\mid p-1 \text{ and } (\frac{a^2+b^2}{p})=1,\\ -\frac{2b}{a}(4a^2+4b^2)^{\frac{p-1}{4}}\left(\frac{2b+2ai}{p}\right)_4 i \pmod p & \text{if } 4\mid p-1 \text{ and } (\frac{a^2+b^2}{p})=-1,\\ 0 \pmod p & \text{if } 4\mid p-3 \text{ and } (\frac{a^2+b^2}{p})=1,\\ \frac{1}{a}(4a^2+4b^2)^{\frac{p+1}{4}}\left(\frac{2b+2ai}{p}\right)_4 i \pmod p & \text{if } 4\mid p-3 \text{ and } (\frac{a^2+b^2}{p})=-1. \end{cases}
\end{aligned}
$$

Clearly $\left(\frac{2b+2ai}{p}\right)_4=\left(\frac{b+ai}{p}\right)_4$. By Lemma 4.1, $\left(\frac{b+ai}{p}\right)_4^2=\left(\frac{a^2+b^2}{p}\right)$. Thus, if $\left(\frac{b+ai}{p}\right)_4=\pm1$, then $\left(\frac{a^2+b^2}{p}\right)=1$; if $\left(\frac{b+ai}{p}\right)_4=\pm i$, then $\left(\frac{a^2+b^2}{p}\right)=-1$. Hence applying (1.3), (1.4) and the above we obtain

$$
\begin{aligned}
(b+\sqrt{a^2+b^2})^{\frac{p-1}{2}} &= \sqrt{a^2+b^2}\,U_{\frac{p-1}{2}}(2b,-a^2)+\frac{1}{2}V_{\frac{p-1}{2}}(2b,-a^2)\\
&\equiv \begin{cases} \pm(2\sqrt{a^2+b^2})^{\frac{p-1}{2}} \pmod p & \text{if } \left(\frac{b+ai}{p}\right)_4=\pm1,\\ \pm\frac{b-\sqrt{a^2+b^2}}{a}(2\sqrt{a^2+b^2})^{\frac{p-1}{2}} \pmod p & \text{if } \left(\frac{b+ai}{p}\right)_4=\pm i. \end{cases}
\end{aligned}
$$

This yields the result.

Remark 4.1 When $\left(\frac{b+ai}{p}\right)_4=\pm1$ (or $\left(\frac{a^2+b^2}{p}\right)=1$), Theorem 4.1 can also be deduced from [Su4, Theorem 2.4]. Note that $\left(\frac{ai}{p}\right)_4=\left(\frac{i}{p}\right)_4=\left(\frac{2}{p}\right)$. We see that the result is true when $p\mid b$. Now assume $p\nmid b$. As $(\frac{a}{b})^2+1=\left(\frac{\sqrt{a^2+b^2}}{b}\right)^2$, by [Su4, Theorem 2.4] we have

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

and so

$$
\begin{aligned}
\left(\frac{b+ai}{p}\right)_4=\left(\frac{b-ai}{p}\right)_4=\left(\frac{i}{p}\right)_4\left(\frac{a+bi}{p}\right)_4=\left(\frac{2}{p}\right)\left(\frac{a+bi}{p}\right)_4\\
=\left(\frac{2\sqrt{a^2+b^2}}{p}\right)\left(\frac{b+\sqrt{a^2+b^2}}{p}\right).
\end{aligned}
$$

This yields the result.

Corollary 4.1. *Let p be an odd prime. Then*

$$
\left(\frac{1+\sqrt2}{\sqrt2}\right)^{\frac{p-1}{2}}\equiv\begin{cases} (-1)^{\frac{p\mp1}{8}} \pmod p & \text{if } p\equiv\pm1 \pmod 8,\\ (-1)^{\frac{p\pm3}{8}}(1-\sqrt2) \pmod p & \text{if } p\equiv\pm5 \pmod 8.\end{cases}
$$

Proof. Taking $a=b=1$ in Theorem 4.1 we obtain

$$\Big(\frac{1+\sqrt{2}}{2\sqrt{2}}\Big)^{\frac{p-1}{2}} \equiv \begin{cases} \pm 1 \pmod p & \text{if } \big(\frac{1+i}{p}\big)_4 = \pm 1, \\ \pm(1-\sqrt{2}) \pmod p & \text{if } \big(\frac{1+i}{p}\big)_4 = \pm i. \end{cases}$$

To see the result, we note that $2^{\frac{p-1}{2}} \equiv (-1)^{\frac{p^2-1}{8}} \pmod p$ and

$$\Big(\frac{1+i}{p}\Big)_4 = i^{\frac{(-1)^{\frac{p-1}{2}}p-1}{4}} = \begin{cases} (-1)^{\frac{p\mp 1}{8}} & \text{if } p \equiv \pm 1 \pmod 8, \\ (-1)^{\frac{p\mp 5}{8}} i & \text{if } p \equiv \pm 5 \pmod 8). \end{cases}$$

Corollary 4.2. *Let $p \neq 2,5$ be a prime. Then*

$$\Big(\frac{1+\sqrt{5}}{2\sqrt{5}}\Big)^{\frac{p-1}{2}} \equiv \begin{cases} 1 \pmod p & \text{if } p \equiv \pm 1 \pmod{20}, \\ -1 \pmod p & \text{if } p \equiv \pm 9 \pmod{20}, \\ \frac{1-\sqrt{5}}{2} \pmod p & \text{if } p \equiv \pm 3 \pmod{20}, \\ \frac{-1+\sqrt{5}}{2} \pmod p & \text{if } p \equiv \pm 7 \pmod{20}. \end{cases}$$

Proof. Set $p^* = (-1)^{\frac{p-1}{2}}p$. Taking $a=2$ and $b=1$ in Theorem 4.1 and noting that

$$\Big(\frac{1+2i}{p}\Big)_4 = \Big(\frac{1+2i}{p^*}\Big)_4 = \Big(\frac{p^*}{1+2i}\Big)_4 = \begin{cases} \pm 1 & \text{if } p^* \equiv \pm 1 \pmod 5, \\ \pm i & \text{if } p^* \equiv \pm 2 \pmod 5 \end{cases}$$

we obtain the result.

Corollary 4.3. *Let $p \neq 2,13$ be a prime. Then*

$$\Big(\frac{3+\sqrt{13}}{2\sqrt{13}}\Big)^{\frac{p-1}{2}} \equiv \begin{cases} 1 \pmod p & \text{if } p \equiv \pm 1, \pm 9, \pm 23 \pmod{52}, \\ -1 \pmod p & \text{if } p \equiv \pm 3, \pm 17, \pm 25 \pmod{52}, \\ \frac{3-\sqrt{13}}{2} \pmod p & \text{if } p \equiv \pm 15, \pm 19, \pm 21 \pmod{52}, \\ \frac{-3+\sqrt{13}}{2} \pmod p & \text{if } p \equiv \pm 5, \pm 7, \pm 11 \pmod{52}. \end{cases}$$

Proof. Set $p^* = (-1)^{\frac{p-1}{2}}p$. Taking $a=2$ and $b=3$ in Theorem 4.1 and noting that

$$\Big(\frac{3+2i}{p}\Big)_4 = \Big(\frac{3+2i}{p^*}\Big)_4 = \Big(\frac{p^*}{3+2i}\Big)_4 = \begin{cases} \pm 1 & \text{if } p^* \equiv \pm 1, \pm 3, \pm 9 \pmod{13}, \\ \pm i & \text{if } p^* \equiv \mp 2, \mp 5, \mp 6 \pmod{13} \end{cases}$$

we deduce the result.

Remark 4.2 Corollaries 4.1-4.3 can also be deduced from [Su2], [SS] and [Su5] respectively.

Corollary 4.4. *Let $p \neq 2, 17$ be a prime. Then*

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

Proof. Using the properties of the quartic Jacobi symbol, one can easily see that

$$\Big(\frac{2}{p}\Big)\Big(\frac{4+i}{p}\Big)_4 = \Big(\frac{2}{p}\Big)\Big(\frac{i}{p}\Big)_4\Big(\frac{1-4i}{p}\Big)_4 = \Big(\frac{1-4i}{p}\Big)_4 = \Big(\frac{p}{1-4i}\Big)_4$$
$$= \begin{cases} 1 & \text{if } p \equiv \pm 1, \pm 4 \pmod{17}, \\ -1 & \text{if } p \equiv \pm 2, \pm 8 \pmod{17}, \\ i & \text{if } p \equiv \pm 3, \pm 5 \pmod{17}, \\ -i & \text{if } p \equiv \pm 6, \pm 7 \pmod{17}. \end{cases}$$

Now taking $a = 1$ and $b = 4$ in Theorem 4.1 and applying the above we obtain the result.

Corollary 4.5. *Let $p \neq 2, 17$ be a prime. Then*

$$U_{\frac{p-1}{2}}(8,-1)$$
$$\equiv \begin{cases} 0 \pmod p & \text{if } p \equiv \pm 1, \pm 2, \pm 4, \pm 8 \pmod{17} \text{ and } 4 \mid p-1, \\ 17^{\frac{p-3}{4}} \pmod p & \text{if } p \equiv \pm 1, \pm 4 \pmod{17} \text{ and } p \equiv 3 \pmod 4, \\ -17^{\frac{p-3}{4}} \pmod p & \text{if } p \equiv \pm 2, \pm 8 \pmod{17} \text{ and } p \equiv 3 \pmod 4, \\ -17^{\frac{p-1}{4}} \pmod p & \text{if } p \equiv \pm 3, \pm 5 \pmod{17} \text{ and } p \equiv 1 \pmod 4, \\ 17^{\frac{p-1}{4}} \pmod p & \text{if } p \equiv \pm 6, \pm 7 \pmod{17} \text{ and } p \equiv 1 \pmod 4, \\ 4 \cdot 17^{\frac{p-3}{4}} \pmod p & \text{if } p \equiv \pm 3, \pm 5 \pmod{17} \text{ and } p \equiv 3 \pmod 4, \\ -4 \cdot 17^{\frac{p-3}{4}} \pmod p & \text{if } p \equiv \pm 6, \pm 7 \pmod{17} \text{ and } p \equiv 3 \pmod 4 \end{cases}$$

and

$$V_{\frac{p-1}{2}}(8,-1)$$
$$\equiv \begin{cases} 0 \pmod p & \text{if } p \equiv \pm 1, \pm 2, \pm 4, \pm 8 \pmod{17} \text{ and } 4 \mid p-3, \\ 2 \cdot 17^{\frac{p-1}{4}} \pmod p & \text{if } p \equiv \pm 1, \pm 4 \pmod{17} \text{ and } p \equiv 1 \pmod 4, \\ -2 \cdot 17^{\frac{p-1}{4}} \pmod p & \text{if } p \equiv \pm 2, \pm 8 \pmod{17} \text{ and } p \equiv 1 \pmod 4, \\ 8 \cdot 17^{\frac{p-1}{4}} \pmod p & \text{if } p \equiv \pm 3, \pm 5 \pmod{17} \text{ and } p \equiv 1 \pmod 4, \\ -2 \cdot 17^{\frac{p+1}{4}} \pmod p & \text{if } p \equiv \pm 3, \pm 5 \pmod{17} \text{ and } p \equiv 3 \pmod 4, \\ -8 \cdot 17^{\frac{p-1}{4}} \pmod p & \text{if } p \equiv \pm 6, \pm 7 \pmod{17} \text{ and } p \equiv 1 \pmod 4, \\ 2 \cdot 17^{\frac{p+1}{4}} \pmod p & \text{if } p \equiv \pm 6, \pm 7 \pmod{17} \text{ and } p \equiv 3 \pmod 4. \end{cases}$$

Proof. From (1.3) and (1.4) we have

$$U_n(8,-1)=\frac{1}{2\sqrt{17}}\{(4+\sqrt{17})^n-(4-\sqrt{17})^n\}$$

and

$$V_n(8,-1)=(4+\sqrt{17})^n+(4-\sqrt{17})^n.$$

Thus applying Corollary 4.4 we obtain the result.

Lemma 4.2. *Let p be an odd prime, $m\in\mathbb{Z}$, $4\nmid m$ and $p\nmid m$. Let $A\in\mathbb{Z}$, $A=2^rA_0(2\nmid A_0)$, $(A,m)=1$ and $p\nmid A$. Suppose $Ap=x^2+my^2$ with $x,y\in\mathbb{Z}$, $(x,y)=1$, $x=2^\alpha x_0$, $y=2^\beta y_0$ and $x_0\equiv y_0\equiv 1 \pmod 4$.*

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

$$m^{\frac{p-1}{4}}\equiv\begin{cases}(-1)^{\frac{p-1}{4}(\alpha+\beta+1)+\frac{r(x_0y_0-1)}{4}}\left(\frac{x_0}{mA_0}\right)\left(\frac{y_0}{A_0}\right)\pmod p & \text{if } 2\nmid m,\\ (-1)^{\frac{p-1}{4}(\alpha+\beta+1)+\frac{x_0-1}{4}}\left(\frac{x_0}{Am/2}\right)\left(\frac{y_0}{A}\right)\pmod p & \text{if } 2\parallel m.\end{cases}$$

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

$$m^{\frac{p-3}{4}}\equiv\begin{cases}-(-1)^{\frac{p+1}{4}(\alpha+\beta+1)+\frac{r(x_0y_0-1)}{4}}\left(\frac{x_0}{mA_0}\right)\left(\frac{y_0}{A_0}\right)\frac{y}{x}\pmod p & \text{if } 2\nmid m,\\ -(-1)^{\frac{p+1}{4}(\alpha+\beta+1)+\frac{x_0-1}{4}}\left(\frac{x_0}{Am/2}\right)\left(\frac{y_0}{A}\right)\frac{y}{x}\pmod p & \text{if } 2\parallel m.\end{cases}$$

Proof. As $(A,m)=1$ and $(x,y)=1$ we see that $(A,x_0)=(A,y_0)=(m,x_0)=1$ and $p\nmid xy$. It is clear that

$$\begin{aligned}\left(\frac{x_0y_0}{p}\right)&=\left(\frac{x_0y_0}{A_0p}\right)\left(\frac{x_0y_0}{A_0}\right)=\left(\frac{A_0p}{x_0y_0}\right)\left(\frac{x_0y_0}{A_0}\right)=\left(\frac{(x^2+my^2)/2^r}{x_0y_0}\right)\left(\frac{x_0y_0}{A_0}\right)\\&=\left(\frac{2^r}{x_0y_0}\right)\left(\frac{my^2}{x_0}\right)\left(\frac{x^2}{y_0}\right)\left(\frac{x_0y_0}{A_0}\right)=\left(\frac{2}{x_0y_0}\right)^r\left(\frac{m}{x_0}\right)\left(\frac{x_0y_0}{A_0}\right)\\&=\begin{cases}\left(\frac{2}{x_0y_0}\right)^r\left(\frac{x_0}{m}\right)\left(\frac{x_0y_0}{A_0}\right)=(-1)^{\frac{r(x_0y_0-1)}{4}}\left(\frac{x_0}{mA_0}\right)\left(\frac{y_0}{A_0}\right) & \text{if } 2\nmid m,\\ \left(\frac{2}{x_0}\right)\left(\frac{m/2}{x_0}\right)\left(\frac{x_0y_0}{A}\right)=(-1)^{\frac{x_0-1}{4}}\left(\frac{x_0}{Am/2}\right)\left(\frac{y_0}{A}\right) & \text{if } 2\parallel m.\end{cases}\end{aligned}$$

Thus

$$\begin{aligned}(x/y)^{\frac{p-1}{2}}&\equiv\left(\frac{x}{p}\right)\left(\frac{y}{p}\right)=\left(\frac{2}{p}\right)^{\alpha+\beta}\left(\frac{x_0y_0}{p}\right)\\&=\begin{cases}\left(\frac{2}{p}\right)^{\alpha+\beta}(-1)^{\frac{r(x_0y_0-1)}{4}}\left(\frac{x_0}{mA_0}\right)\left(\frac{y_0}{A_0}\right)\pmod p & \text{if } 2\nmid m,\\ \left(\frac{2}{p}\right)^{\alpha+\beta}(-1)^{\frac{x_0-1}{4}}\left(\frac{x_0}{Am/2}\right)\left(\frac{y_0}{A}\right)\pmod p & \text{if } 2\parallel m.\end{cases}\end{aligned}$$

If $p\equiv 1\pmod 4$, then $\left(\frac{2}{p}\right)=(-1)^{\frac{p-1}{4}}$ and $m^{\frac{p-1}{4}}=(-1)^{\frac{p-1}{4}}(-m)^{\frac{p-1}{4}}\equiv(-1)^{\frac{p-1}{4}}(x/y)^{\frac{p-1}{2}}\pmod p$. If $p\equiv 3\pmod 4$, then $\left(\frac{2}{p}\right)=(-1)^{\frac{p+1}{4}}$ and

$m^{\frac{p-3}{4}} = (-1)^{\frac{p-3}{4}}(-m)^{\frac{p-3}{4}} \equiv -(-1)^{\frac{p+1}{4}}(x/y)^{\frac{p-3}{2}} = -(-1)^{\frac{p+1}{4}}(x/y)^{\frac{p-1}{2}}\frac{y}{x}$ (mod p).

Now putting all the above together we obtain the result.

For an odd prime p and $m \in \mathbb{Z}$ with $(\frac{-m}{p}) = 1$, from the theory of binary quadratic forms we know that p can be represented by some form $Ax^2+2Bxy+Cy^2$ of discriminant $-4m$, where $A, B, C \in \mathbb{Z}$ and A is coprime to a given positive integer. See [Su6, Lemma 3.1].

Theorem 4.2. *Let p be an odd prime, $m \in \mathbb{Z}$, $4 \nmid m$ and $p \nmid m$. Suppose $p = Ax^2 + 2Bxy + Cy^2$ with $A, B, C, x, y \in \mathbb{Z}$, $p \nmid A$, $(A, 2m) = 1$ and $(2B)^2 - 4AC = -4m$. Assume $Ax + By = 2^\alpha x_0$, $y = 2^\beta y_0$ and $x_0 \equiv y_0 \equiv 1 \pmod 4$.*

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

$$m^{\frac{p-1}{4}} \equiv \begin{cases} (-1)^{\frac{(m-1)y^2-A+1}{4}}\left(\frac{Ax+By}{m}\right)\left(\frac{B}{A}\right) \pmod p & \text{if } 2 \nmid m, \\ (-1)^{\frac{p-1+A-A^2+Amy^2}{8}}\left(\frac{Ax+By}{m/2}\right)\left(\frac{B}{A}\right) \pmod p & \text{if } 2 \parallel m. \end{cases}$$

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

$$m^{\frac{p-3}{4}} \equiv \begin{cases} (-1)^{\frac{(m-1)y^2+A-3}{4}}\left(\frac{Ax+By}{m}\right)\left(\frac{B}{A}\right)\frac{y}{Ax+By} \pmod p & \text{if } 2 \nmid m, \\ (-1)^{\frac{p-5+A-A^2+Amy^2}{8}}\left(\frac{Ax+By}{m/2}\right)\left(\frac{B}{A}\right)\frac{y}{Ax+By} \pmod p & \text{if } 2 \parallel m. \end{cases}$$

Proof. Set $x_1 = Ax + By$. Then clearly $Ap = A^2x^2 + 2ABxy + ACy^2 = (Ax + By)^2 + (AC - B^2)y^2 = x_1^2 + my^2$. As $(A, m) = 1$ and $m = AC - B^2$ we have $(A, B) = 1$. Since $(A, y) \mid p$ and $p \nmid A$ we have $(A, y) = 1$. Thus $(A, x_1) = (A, By) = 1$. As $(m, x_1) \mid Ap$, $p \nmid m$ and $(A, m) = 1$, we see that $(m, x_1) = 1$. Since $x_1^2 + my^2 = Ap \not\equiv 0 \pmod{p^2}$ and $(x, y) \mid p$ we have $p \nmid x_1 y$ and $(x_1, y) = (Ax, y) = (x, y) = 1$.

We first assume $2 \nmid m$. It is clear that

$$\begin{aligned}\left(\frac{2}{p}\right)^{\alpha+\beta}\left(\frac{x_0}{mA}\right)\left(\frac{y_0}{A}\right) &= \left(\frac{2}{p}\right)^{\alpha+\beta}\left(\frac{2}{mA}\right)^{\alpha}\left(\frac{Ax+By}{mA}\right)\left(\frac{2}{A}\right)^{\beta}\left(\frac{y}{A}\right) \\ &= \left(\frac{2}{Ap}\right)^{\alpha+\beta}\left(\frac{2}{m}\right)^{\alpha}\left(\frac{Ax+By}{m}\right)\left(\frac{By}{A}\right)\left(\frac{y}{A}\right) \\ &= \left(\frac{2}{x_1^2+my^2}\right)^{\alpha+\beta}\left(\frac{2}{m}\right)^{\alpha}\left(\frac{Ax+By}{m}\right)\left(\frac{B}{A}\right).\end{aligned}$$

As $x_1^2 + y^2 \equiv x_1^2 + my^2 = Ap \equiv 1 \pmod 2$, we see that $x_1 + y \equiv 1 \pmod 2$. If $2 \mid x_1$, then $2 \nmid y$, $y^2 \equiv 1 \pmod 8$ and so

$$\begin{aligned}\left(\frac{2}{x_1^2+my^2}\right) &= \left(\frac{2}{x_1^2+m}\right) = \left(\frac{2}{m}\right)\left(\frac{2}{mx_1^2+m^2}\right) = \left(\frac{2}{m}\right)\left(\frac{2}{mx_1^2+1}\right) \\ &= (-1)^{\frac{mx_1^2(mx_1^2+2)}{8}}\left(\frac{2}{m}\right) = (-1)^{\frac{mx_1^2}{4}(m\frac{x_1^2}{2}+1)}\left(\frac{2}{m}\right) = (-1)^{\frac{x_1}{2}}\left(\frac{2}{m}\right).\end{aligned}$$

If $2 \nmid x_1$, then $2 \mid y$, $x_1^2 \equiv 1 \pmod 8$ and thus

$$\Big(\frac{2}{x_1^2+my^2}\Big) = \Big(\frac{2}{1+my^2}\Big) = (-1)^{\frac{my^2(my^2+2)}{8}} = (-1)^{\frac{my^2}{4}(m\frac{y^2}{2}+1)} = (-1)^{\frac{y}{2}}.$$

Hence

$$\Big(\frac{2}{x_1^2+my^2}\Big)^{\alpha+\beta}\Big(\frac{2}{m}\Big)^{\alpha} = \begin{cases} \big(\frac{2}{m}\big)^{\alpha}\big(\frac{2}{x_1^2+my^2}\big)^{\alpha} = (-1)^{\frac{x_1}{2}\alpha} = (-1)^{\frac{x_1}{2}} & \text{if } 2 \mid x_1, \\ \big(\frac{2}{x_1^2+my^2}\big)^{\beta} = (-1)^{\frac{y}{2}\beta} = (-1)^{\frac{y}{2}} & \text{if } 2 \nmid x_1 \end{cases}$$
$$= (-1)^{\frac{x_1 y}{2}}$$

and therefore

$$\text{(4.1)} \qquad \Big(\frac{2}{p}\Big)^{\alpha+\beta}\Big(\frac{x_0}{mA}\Big)\Big(\frac{y_0}{A}\Big) = (-1)^{\frac{x_1 y}{2}}\Big(\frac{x_1}{m}\Big)\Big(\frac{B}{A}\Big).$$

If $p \equiv 1 \pmod 4$, then

$$\begin{aligned}(-1)^{\frac{p-1}{4}+\frac{x_1 y}{2}} &= (-1)^{\frac{Ap-A}{4}+\frac{x_1 y}{2}} = (-1)^{\frac{x_1^2+my^2-A}{4}+\frac{2x_1 y}{4}} \\ &= (-1)^{\frac{(x_1+y)^2-1}{4}+\frac{(m-1)y^2-A+1}{4}} = (-1)^{\frac{(m-1)y^2-A+1}{4}}.\end{aligned}$$

This together with Lemma 4.2 and (4.1) yields

$$\begin{aligned}m^{\frac{p-1}{4}} &\equiv (-1)^{\frac{p-1}{4}}\Big(\frac{2}{p}\Big)^{\alpha+\beta}\Big(\frac{x_0}{mA}\Big)\Big(\frac{y_0}{A}\Big) = (-1)^{\frac{p-1}{4}+\frac{x_1 y}{2}}\Big(\frac{x_1}{m}\Big)\Big(\frac{B}{A}\Big) \\ &= (-1)^{\frac{(m-1)y^2-A+1}{4}}\Big(\frac{x_1}{m}\Big)\Big(\frac{B}{A}\Big) \pmod p.\end{aligned}$$

Similarly, if $p \equiv 3 \pmod 4$, then

$$\begin{aligned}(-1)^{\frac{p+1}{4}+\frac{x_1 y}{2}} &= (-1)^{\frac{Ap+A}{4}+\frac{x_1 y}{2}} = (-1)^{\frac{x_1^2+my^2+A}{4}+\frac{2x_1 y}{4}} \\ &= (-1)^{\frac{(x_1+y)^2-1}{4}+\frac{(m-1)y^2+A+1}{4}} = (-1)^{\frac{(m-1)y^2+A+1}{4}}.\end{aligned}$$

By Lemma 4.2 and (4.1) we have

$$\begin{aligned}m^{\frac{p-3}{4}} &\equiv -(-1)^{\frac{p+1}{4}}\Big(\frac{2}{p}\Big)^{\alpha+\beta}\Big(\frac{x_0}{mA}\Big)\Big(\frac{y_0}{A}\Big)\frac{y}{x_1} = -(-1)^{\frac{p+1}{4}+\frac{x_1 y}{2}}\Big(\frac{x_1}{m}\Big)\Big(\frac{B}{A}\Big)\frac{y}{x_1} \\ &= (-1)^{\frac{(m-1)y^2+A-3}{4}}\Big(\frac{x_1}{m}\Big)\Big(\frac{B}{A}\Big)\frac{y}{x_1} \pmod p.\end{aligned}$$

Now we assume $2 \parallel m$. As $x_1^2 \equiv x_1^2+my^2 = Ap \equiv 1 \pmod 2$ we have $2 \nmid x_1$ and so $\alpha = 0$. When $2 \mid y$ we have $Ap = x_1^2+my^2 \equiv x_1^2 \equiv 1 \pmod 8$ and so

$\left(\frac{2}{Ap}\right)=1$. Since $Ap=x_1^2+my^2$ and $A^2p=(A^2-1)(p-1)+p+A^2-1\equiv p-1+A^2 \pmod{16}$ we see that

$$\begin{aligned}&(-1)^{\frac{x_1^2-1}{8}+\frac{p-(-1)^{\frac{p-1}{2}}}{4}}\\ &=(-1)^{\frac{Ap-my^2-1}{8}+\frac{2p-2(-1)^{\frac{p-1}{2}}}{8}}=(-1)^{\frac{-A^2p+Amy^2+A}{8}+\frac{2p-2(-1)^{\frac{p-1}{2}}}{8}}\\ &=(-1)^{\frac{-(p-1+A^2)+Amy^2+A+2p-2(-1)^{\frac{p-1}{2}}}{8}}=(-1)^{\frac{p+1-A^2+A-2(-1)^{\frac{p-1}{2}}+Amy^2}{8}}.\end{aligned}$$

Thus

$$\begin{aligned}&\left(\frac{2}{p}\right)^{\alpha+\beta+1}(-1)^{\frac{x_0-1}{4}}\left(\frac{x_0}{Am/2}\right)\left(\frac{y_0}{A}\right)\\ &=(-1)^{\frac{x_1-1}{4}}\left(\frac{2}{p}\right)^{\beta+1}\left(\frac{x_1}{Am/2}\right)\left(\frac{2}{A}\right)^{\beta}\left(\frac{y}{A}\right)\\ &=(-1)^{\frac{x_1-1}{4}}\left(\frac{2}{p}\right)\left(\frac{2}{Ap}\right)^{\beta}\left(\frac{x_1}{m/2}\right)\left(\frac{By}{A}\right)\left(\frac{y}{A}\right)\\ &=(-1)^{\frac{x_1^2-1}{8}+\frac{p-(-1)^{\frac{p-1}{2}}}{4}}\left(\frac{x_1}{m/2}\right)\left(\frac{B}{A}\right)\\ &=(-1)^{\frac{p+1-A^2+A-2(-1)^{\frac{p-1}{2}}+Amy^2}{8}}\left(\frac{x_1}{m/2}\right)\left(\frac{B}{A}\right).\end{aligned}$$

This together with Lemma 4.2 yields the result. Hence the theorem is proved.

Corollary 4.6. *Let p be an odd 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.*

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

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

(ii) *If $p\equiv 3\pmod 4$ and we choose the sign of y so that $y\equiv 1\pmod 4$, then*

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

Proof. Let $x_1\in\{x,-x\}$ be such that $x_1=2^{\alpha}x_0$ and $x_0\equiv 1\pmod 4$. We first assume $p\equiv 1\pmod 4$. Taking $A=1$, $B=0$ and $C=m$ in Theorem 4.2 we have

$$m^{\frac{p-1}{4}}\equiv\begin{cases}(-1)^{\frac{(m-1)y^2}{4}}\left(\frac{x_1}{m}\right)\pmod p & \text{if } 2\nmid m,\\ (-1)^{\frac{p-1+my^2}{8}}\left(\frac{x_1}{m/2}\right)\pmod p & \text{if } 2\parallel m.\end{cases}\tag{4.2}$$

If $m\equiv 3\pmod 4$, then $2\nmid x$, $2\mid y$ and so $(-1)^{\frac{(m-1)y^2}{4}}=1$. Thus, by (4.2) we have $m^{\frac{p-1}{4}}\equiv \big(\frac{(-1)^{\frac{x-1}{2}}x}{m}\big)=(-1)^{\frac{x-1}{2}}\big(\frac{x}{m}\big)\pmod p$. If $m\equiv 1\pmod 8$, then $\big(\frac{x}{m}\big)=\big(\frac{-x}{m}\big)$. Thus, by (4.2) we have $m^{\frac{p-1}{4}}\equiv\big(\frac{x_1}{m}\big)=\big(\frac{x}{m}\big)\pmod p$. If $m\equiv 5\pmod 8$, then $\big(\frac{x}{m}\big)=\big(\frac{-x}{m}\big)$ and $(-1)^y=(-1)^{x-1}$. Thus, by (4.2) we have $m^{\frac{p-1}{4}}\equiv(-1)^y\big(\frac{x_1}{m}\big)=(-1)^{x-1}\big(\frac{x}{m}\big)\pmod p$. If $m\equiv 2\pmod 4$, we have $2\mid y$ and $p\equiv x^2\equiv 1\pmod 8$. Thus, by (4.2) we have

$$\begin{aligned}m^{\frac{p-1}{4}}&\equiv(-1)^{\frac{p-1+my^2}{8}}\Big(\frac{x_1}{m/2}\Big)=(-1)^{\frac{p-1-my^2}{8}}\Big(\frac{(-1)^{\frac{x-1}{2}}x}{m/2}\Big)\\&=(-1)^{\frac{x^2-1}{8}+\frac{m-2}{4}\cdot\frac{x-1}{2}}\Big(\frac{x}{m/2}\Big)\pmod p.\end{aligned}$$

Now assume $p\equiv 3\pmod 4$. Then clearly $m\equiv 2,3\pmod 4$ and $2\nmid y$. We may choose the sign of y so that $y\equiv 1\pmod 4$. Taking $A=1$, $B=0$ and $C=m$ in Theorem 4.2(ii) we have

$$(4.3)\qquad m^{\frac{p-3}{4}}\equiv\begin{cases}(-1)^{\frac{(m-1)y^2-2}{4}}\big(\frac{x_1}{m}\big)\frac{y}{x_1}\pmod p & \text{if } m\equiv 3\pmod 4,\\ (-1)^{\frac{p-5+my^2}{8}}\big(\frac{x_1}{m/2}\big)\frac{y}{x_1}\pmod p & \text{if } m\equiv 2\pmod 4.\end{cases}$$

If $m\equiv 3\pmod 4$, as $y^2\equiv 1\pmod 8$ and $\big(\frac{x}{m}\big)\frac{1}{x}=\big(\frac{-x}{m}\big)\frac{1}{-x}$ we have $m^{\frac{p-3}{4}}\equiv(-1)^{\frac{m-3}{4}}\big(\frac{x_1}{m}\big)\frac{y}{x_1}=(-1)^{\frac{m-3}{4}}\big(\frac{x}{m}\big)\frac{y}{x}\pmod p$. If $m\equiv 2\pmod 4$, then $2\nmid xy$ and $my^2=m(y^2-1)+m\equiv m\pmod{16}$. Thus, by (4.3) we have

$$\begin{aligned}m^{\frac{p-3}{4}}&\equiv(-1)^{\frac{p-5+my^2}{8}}\Big(\frac{x_1}{m/2}\Big)\frac{y}{x_1}=(-1)^{\frac{x^2-5+2my^2}{8}}\Big(\frac{x_1}{m/2}\Big)\frac{y}{x_1}\\&=(-1)^{\frac{m-2}{4}+\frac{x^2-1}{8}}\Big(\frac{(-1)^{\frac{x-1}{2}}x}{m/2}\Big)\frac{y}{(-1)^{\frac{x-1}{2}}x}\\&=(-1)^{\frac{m-2}{4}+\frac{x^2-1}{8}+\frac{x-1}{2}+\frac{x-1}{2}\cdot\frac{m-2}{4}}\Big(\frac{x}{m/2}\Big)\frac{y}{x}\\&=(-1)^{\frac{x+1}{2}\cdot\frac{m+2}{4}-1+\frac{x^2-1}{8}}\Big(\frac{x}{m/2}\Big)\frac{y}{x}\pmod p.\end{aligned}$$

This completes the proof.

As examples, if p is an odd prime, we then have

$$\begin{aligned}
2^{\frac{p-1}{4}} &\equiv (-1)^{\frac{x^2-1}{8}} \pmod p \quad \text{for} \quad p = x^2+2y^2 \equiv 1 \pmod 8,\\
2^{\frac{p-3}{4}} &\equiv (-1)^{\frac{x-1}{2}+\frac{x^2-1}{8}} \frac{y}{x} \pmod p \quad \text{for} \quad p = x^2+2y^2 \equiv 3 \pmod 8\\
&\qquad\qquad\qquad\qquad \text{with} \quad y \equiv 1 \pmod 4,\\
3^{\frac{p-1}{4}} &\equiv (-1)^{\frac{x-1}{2}} \Big(\frac{x}{3}\Big) \pmod p \quad \text{for} \quad p = x^2+3y^2 \equiv 1 \pmod{12},\\
3^{\frac{p-3}{4}} &\equiv \Big(\frac{x}{3}\Big)\frac{y}{x} \pmod p \quad \text{for} \quad p = x^2+3y^2 \equiv 7 \pmod{12}\\
&\qquad\qquad\qquad\qquad \text{with} \quad y \equiv 1 \pmod 4,\\
5^{\frac{p-1}{4}} &\equiv (-1)^{x-1} \Big(\frac{x}{5}\Big) \pmod p \quad \text{for} \quad p = x^2+5y^2 \equiv 1,9 \pmod{20}
\end{aligned}$$

and

$$\begin{aligned}
6^{\frac{p-1}{4}} &\equiv (-1)^{\frac{x-1}{2}+\frac{x^2-1}{8}} \Big(\frac{x}{3}\Big) \pmod p \quad \text{for} \quad p = x^2+6y^2 \equiv 1 \pmod{24},\\
6^{\frac{p-3}{4}} &\equiv (-1)^{\frac{x^2-1}{8}-1} \Big(\frac{x}{3}\Big)\frac{y}{x} \pmod p \quad \text{for} \quad p = x^2+6y^2 \equiv 7 \pmod{24}\\
&\qquad\qquad\qquad\qquad \text{with} \quad y \equiv 1 \pmod 4,\\
7^{\frac{p-1}{4}} &\equiv (-1)^{\frac{x-1}{2}} \Big(\frac{x}{7}\Big) \pmod p \quad \text{for} \quad p = x^2+7y^2 \equiv 1,9,25 \pmod{28},\\
7^{\frac{p-3}{4}} &\equiv -\Big(\frac{x}{7}\Big)\frac{y}{x} \pmod p \quad \text{for} \quad p = x^2+7y^2 \equiv 11,15,23 \pmod{28}\\
&\qquad\qquad\qquad\qquad \text{with} \quad y \equiv 1 \pmod 4,\\
10^{\frac{p-1}{4}} &\equiv (-1)^{\frac{x^2-1}{8}} \Big(\frac{x}{5}\Big) \pmod p \quad \text{for} \quad p = x^2+10y^2 \equiv 1,9 \pmod{40},\\
10^{\frac{p-3}{4}} &\equiv (-1)^{\frac{x-1}{2}+\frac{x^2-1}{8}} \Big(\frac{x}{5}\Big)\frac{y}{x} \pmod p \quad \text{for} \quad p = x^2+10y^2 \equiv 11,19 \pmod{40}\\
&\qquad\qquad\qquad\qquad \text{with} \quad y \equiv 1 \pmod 4.
\end{aligned}$$

Remark 4.3 Let p be an odd prime. When $p = x^2+3y^2 \equiv 1 \pmod{12}$, the congruence $3^{\frac{p-1}{4}} \equiv (-1)^{\frac{x-1}{2}}\big(\frac{x}{3}\big) \pmod p$ was proved by Hudson and Williams [HW] using cyclotomic numbers of order 6. When $m \in \{2,3,6\}$ and $p = x^2+my^2 \equiv 3 \pmod 4$, the above congruences for $m^{\frac{p-3}{4}} \pmod p$ have been given in [Lem2, p. 180].

If p and m are distinct primes such that $p \equiv m \equiv 1 \pmod 4$ and $p = x^2+my^2 (x,y \in \mathbb{Z})$. Then $\big(\frac{m}{p}\big) = \big(\frac{p}{m}\big) = \big(\frac{x^2}{m}\big) = 1$ and $\big[\frac{p}{m}\big]_4 = \big(\frac{x}{m}\big)$. Thus, by Corollary 4.6(i) we have

$$\Big[\frac{m}{p}\Big]_4\Big[\frac{p}{m}\Big]_4 = \begin{cases} 1 & \text{if } m \equiv 1 \pmod 8,\\ (-1)^{x-1} = (-1)^y & \text{if } m \equiv 5 \pmod 8. \end{cases}$$

This is a classical result due to Brown [Bro1] and Lehmer [Le3].

Theorem 4.3. *Let p be an odd prime, $m \in \mathbb{Z}$, $2 \nmid m$ and $p \nmid m$.*

(i) *If $p \equiv 1 \pmod 4$ and $2p = x^2 + my^2$ for $x, y \in \mathbb{Z}$, then $m^{\frac{p-1}{4}} \equiv (-1)^{\frac{m-1}{8}} \left(\frac{x}{m}\right) \pmod p$.*

(ii) *If $p \equiv 3 \pmod 4$ and $2p = x^2 + my^2$ with $x, y \in \mathbb{Z}$ and $4 \mid x - y$, then $m^{\frac{p-3}{4}} \equiv (-1)^{\frac{m-5}{8}} \left(\frac{x}{m}\right) \frac{y}{x} \pmod p$.*

(iii) *If $p \equiv 1 \pmod 4$ and $4p = x^2 + my^2$ for $x, y \in \mathbb{Z}$, then $(-m)^{\frac{p-1}{4}} \equiv (-1)^{\frac{x-1}{2}} \left(\frac{x}{m}\right) \pmod p$.*

(iv) *If $p \equiv 3 \pmod 4$ and $4p = x^2 + my^2$ with $x, y \in \mathbb{Z}$ and $4 \mid x - y$, then $(-m)^{\frac{p-3}{4}} \equiv (-1)^{\frac{x-1}{2}} \left(\frac{x}{m}\right) \frac{y}{x} \pmod p$.*

Proof. As $2 \nmid xy$ we may assume $x \equiv y \equiv 1 \pmod 4$. We first assume $2p = x^2 + my^2$. Then $2p \equiv 1 + m \pmod 8$ and so $p \equiv 1$ or $3 \pmod 4$ according as $m \equiv 1$ or $5 \pmod 8$. If $p \equiv 1 \pmod 4$, taking $A = 2$ in Lemma 4.2(i) we see that $m^{\frac{p-1}{4}} \equiv (-1)^{\frac{p-1}{4} + \frac{xy-1}{4}} \left(\frac{x}{m}\right) \pmod p$. Clearly

$$\begin{aligned}(-1)^{\frac{p-1}{4} + \frac{xy-1}{4}} &= (-1)^{\frac{x^2+my^2-2}{8} + \frac{xy-1}{4}} = (-1)^{\frac{(x-y)^2+2xy+(m-1)y^2-2}{8} + \frac{xy-1}{4}} \\ &= (-1)^{\frac{xy+\frac{m-1}{2}y^2-1}{4} + \frac{xy-1}{4}} = (-1)^{\frac{m-1}{8}y^2} = (-1)^{\frac{m-1}{8}}.\end{aligned}$$

Thus (i) is true. If $p \equiv 3 \pmod 4$, then

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

Thus applying Lemma 4.2(ii) we obtain

$$m^{\frac{p-3}{4}} \equiv -(-1)^{\frac{p+1}{4} + \frac{xy-1}{4}} \left(\frac{x}{m}\right) \frac{y}{x} = (-1)^{\frac{m-5}{8}} \left(\frac{x}{m}\right) \frac{y}{x} \pmod p.$$

This proves (ii).

Now assume $4p = x^2 + my^2$. Then $1 + m \equiv x^2 + my^2 = 4p \equiv 4 \pmod 8$ and hence $m \equiv 3 \pmod 8$. Taking $A = 4$ in Lemma 4.2 we deduce (iii) and (iv). So the theorem is proved.

Corollary 4.7. *Let p be a prime such that $p \equiv 3, 7 \pmod{20}$ and hence $2p = x^2 + 5y^2$ for some integers x and y. Suppose $4 \mid x - y$. Then*

$$5^{\frac{p-3}{4}} \equiv \begin{cases} \frac{y}{x} \pmod p & \text{if } p \equiv 3 \pmod{20}, \\ -\frac{y}{x} \pmod p & \text{if } p \equiv 7 \pmod{20}, \end{cases}$$

$$L_{\frac{p-1}{2}} \equiv \frac{x}{y} \pmod p \quad \text{and} \quad F_{\frac{p-1}{2}} \equiv -\frac{1}{2} F_{\frac{p+1}{2}} \equiv \frac{y}{x} \pmod p.$$

Proof. As $x^2 \equiv 2p \pmod 5$ we see that $\left(\frac{x}{5}\right) = 1$ or -1 according as $p \equiv 3 \pmod{20}$ or $p \equiv 7 \pmod{20}$. Thus taking $m = 5$ in Theorem 4.3(ii) we deduce the result for $5^{\frac{p-3}{4}} \pmod p$. By the above and [SS, Corollaries 1 and 2] we have

$$L_{\frac{p-1}{2}} \equiv \begin{cases} -5^{\frac{p+1}{4}} \equiv -5\frac{y}{x} \equiv \frac{x}{y} \pmod p & \text{if } p \equiv 3 \pmod{20}, \\ 5^{\frac{p+1}{4}} \equiv -5\frac{y}{x} \equiv \frac{x}{y} \pmod p & \text{if } p \equiv 7 \pmod{20} \end{cases}$$

and

$$F_{\frac{p-1}{2}} \equiv -\frac{1}{2}F_{\frac{p+1}{2}} \equiv \begin{cases} 5^{\frac{p-3}{4}} \equiv \frac{y}{x} \pmod p & \text{if } p \equiv 3 \pmod{20}, \\ -5^{\frac{p-3}{4}} \equiv \frac{y}{x} \pmod p & \text{if } p \equiv 7 \pmod{20}. \end{cases}$$

This completes the proof.

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*

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

Proof. Suppose $x = 2^\alpha x_0 (2 \nmid x_0)$. Using Lemma 4.1 and [Su6, (2.7) and (2.8)] we see that

$$\begin{aligned}\Big(\frac{x^2}{a+bi}\Big)_4 &= \Big(\frac{2}{a+bi}\Big)_4^{2\alpha}\Big(\frac{x_0^2}{a+bi}\Big)_4 = (-1)^{\frac{b}{2}\alpha}\Big(\frac{a+bi}{x_0^2}\Big)_4 \\ &= (-1)^{\frac{b}{2}\alpha}\Big(\frac{a+bi}{|x_0|}\Big)_4^2 = \Big(\frac{2}{a^2+b^2}\Big)^\alpha\Big(\frac{a^2+b^2}{|x_0|}\Big) \\ &= \Big(\frac{2^\alpha}{a^2+b^2}\Big)\Big(\frac{x_0}{a^2+b^2}\Big) = \Big(\frac{x}{a^2+b^2}\Big).\end{aligned}$$

This proves the lemma.

Remark 4.4 Let $a, b, c, d \in \mathbb{Z}$ with $2 \nmid c$, $2 \mid d$, $(c, d) = 1$ and $(a^2+b^2, c^2+d^2) = 1$. Using Lemma 4.3 we have

$$\begin{aligned}\Big(\frac{a+bi}{c+di}\Big)_4^2 &= \Big(\frac{(ac+bci)^2c^2}{c+di}\Big)_4 = \Big(\frac{(ac+bd)^2c^2}{c+di}\Big)_4 = \Big(\frac{(ac+bd)c}{c^2+d^2}\Big) \\ &= \Big(\frac{ac+bd}{c^2+d^2}\Big)\Big(\frac{c^2+d^2}{c}\Big) = \Big(\frac{ac+bd}{c^2+d^2}\Big).\end{aligned}$$

Theorem 4.4. *Let p be an odd prime and $a, b \in \mathbb{Z}$ with $p \nmid a(a^2+b^2)$ and $4 \nmid a^2+b^2$. Suppose $p = Ax^2+2Bxy+Cy^2$ with $A, B, C, x, y \in \mathbb{Z}$, $p \nmid A$, $(A, 2(a^2+b^2)) = 1$ and $(2B)^2 - 4AC = -4(a^2+b^2)$. Assume $y/2^{\mathrm{ord}_2 y} \equiv (Ax+By)/2^{\mathrm{ord}_2(Ax+By)} \equiv 1 \pmod 4$.*

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

$$\Big(\frac{(b+\sqrt{a^2+b^2})/2}{p}\Big) = \begin{cases} (-1)^{\frac a2 y+\frac{A-1}{4}}\big(\frac BA\big)\big(\frac{b-ai}{A}\big)_4 & \text{if } 2\mid a \text{ and } 2\nmid b,\\ (-1)^{\frac{p-A}{4}+\frac b2 y}\big(\frac BA\big)\big(\frac{a+bi}{A}\big)_4 & \text{if } 2\nmid a \text{ and } 2\mid b,\\ (-1)^{\frac y2} i^{\frac{A-1}{4}}\big(\frac BA\big)\big(\frac{\frac{a+b}{2}-\frac{a-b}{2}i}{A}\big)_4 & \text{if } 2\nmid ab,\ 4\mid a-b \text{ and } 2\mid y,\\ i^{\frac{3-A}{4}}\big(\frac BA\big)\big(\frac{\frac{a+b}{2}-\frac{a-b}{2}i}{A}\big)_4 & \text{if } 2\nmid ab,\ 4\mid a-b \text{ and } 2\nmid y.\end{cases}$$

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

$$\Big(\frac{b+\sqrt{a^2+b^2}}{2}\Big)^{\frac{p-1}{2}} \equiv \begin{cases} (-1)^{\frac a2 y+\frac{A-3}{4}}\big(\frac BA\big)\big(\frac{b-ai}{A}\big)_4 i^{\frac{y}{Ax+By}}\cdot\frac{a^2+b^2-b\sqrt{a^2+b^2}}{a} \pmod p\\ \qquad\qquad \text{if } 2\mid a \text{ and } 2\nmid b,\\ (-1)^{\frac{p-A}{4}+1+\frac b2 y}\big(\frac BA\big)\big(\frac{a+bi}{A}\big)_4 i^{\frac{y}{Ax+By}}\cdot\frac{a^2+b^2-b\sqrt{a^2+b^2}}{a} \pmod p\\ \qquad\qquad \text{if } 2\nmid a \text{ and } 2\mid b,\\ (-1)^{\frac y2+1} i^{\frac{3-A}{4}}\big(\frac BA\big)\big(\frac{\frac{a+b}{2}-\frac{a-b}{2}i}{A}\big)_4 \frac{y}{Ax+By}\cdot\frac{a^2+b^2-b\sqrt{a^2+b^2}}{a} \pmod p\\ \qquad\qquad \text{if } 2\nmid ab,\ 4\mid a-b \text{ and } 2\mid y,\\ i^{\frac{A-1}{4}}\big(\frac BA\big)\big(\frac{\frac{a+b}{2}-\frac{a-b}{2}i}{A}\big)_4 \frac{y}{Ax+By}\cdot\frac{a^2+b^2-b\sqrt{a^2+b^2}}{a} \pmod p\\ \qquad\qquad \text{if } 2\nmid ab,\ 4\mid a-b \text{ and } 2\nmid y.\end{cases}$$

Proof. As $Ap=(Ax+By)^2+(a^2+b^2)y^2$ we see that $\big(\frac{-(a^2+b^2)}{p}\big)=1$ and so $\big(\frac{b+ai}{p}\big)_4^2=\big(\frac{a^2+b^2}{p}\big)=(-1)^{\frac{p-1}{2}}$ by Lemma 4.1. Hence, if $p\equiv 1 \pmod 4$, then $\big(\frac{b+ai}{p}\big)_4=\pm 1$; if $p\equiv 3 \pmod 4$, then $\big(\frac{b+ai}{p}\big)_4=\pm i$. Thus applying Theorem 4.1 we have

(4.4)

$$\Big(\frac{b+\sqrt{a^2+b^2}}{2}\Big)^{\frac{p-1}{2}} \equiv \begin{cases} (a^2+b^2)^{\frac{p-1}{4}}\big(\frac{b+ai}{p}\big)_4 \pmod p & \text{if } p\equiv 1 \pmod 4,\\ -\sqrt{a^2+b^2}(a^2+b^2)^{\frac{p-3}{4}}\frac{b-\sqrt{a^2+b^2}}{a}\big(\frac{b+ai}{p}\big)_4 i \pmod p & \text{if } p\equiv 3 \pmod 4.\end{cases}$$

Now we consider the following three cases.

Case 1. $2\mid a$ and $2\nmid b$. In this case, $Ap=(Ax+By)^2+(a^2+b^2)y^2\equiv (Ax+By)^2+y^2\equiv 1 \pmod 4$ and

$$a^2+b^2\equiv a^2+1\equiv \begin{cases} 1 \pmod 8 & \text{if } 4\mid a,\\ 5 \pmod 8 & \text{if } 2\parallel a.\end{cases}$$

Thus, if $p \equiv 1 \pmod 4$, by Theorem 4.2(i) we have

$$(a^2+b^2)^{\frac{p-1}{4}} \equiv (-1)^{\frac{a}{2}y+\frac{A-1}{4}} \Big(\frac{Ax+By}{a^2+b^2}\Big)\Big(\frac{B}{A}\Big) \pmod p;$$

if $p \equiv 3 \pmod 4$, by Theorem 4.2(ii) we have

$$(a^2+b^2)^{\frac{p-3}{4}} \equiv (-1)^{\frac{a}{2}y+\frac{A-3}{4}} \Big(\frac{Ax+By}{a^2+b^2}\Big)\Big(\frac{B}{A}\Big)\frac{y}{Ax+By} \pmod p.$$

On the other hand, using Lemma 4.3 we have

$$\begin{aligned}\Big(\frac{b+ai}{p}\Big)_4 &= \Big(\frac{b+ai}{A}\Big)_4^{-1}\Big(\frac{b+ai}{Ap}\Big)_4 = \Big(\frac{b-ai}{A}\Big)_4\Big(\frac{Ap}{b+ai}\Big)_4 \\ &= \Big(\frac{b-ai}{A}\Big)_4\Big(\frac{(Ax+By)^2+(a^2+b^2)y^2}{b+ai}\Big)_4 \\ &= \Big(\frac{b-ai}{A}\Big)_4\Big(\frac{(Ax+By)^2}{b+ai}\Big)_4 = \Big(\frac{b-ai}{A}\Big)_4\Big(\frac{Ax+By}{a^2+b^2}\Big).\end{aligned}$$

Hence, if $p \equiv 1 \pmod 4$, then

$$(a^2+b^2)^{\frac{p-1}{4}}\Big(\frac{b+ai}{p}\Big)_4 \equiv (-1)^{\frac{a}{2}y+\frac{A-1}{4}}\Big(\frac{B}{A}\Big)\Big(\frac{b-ai}{A}\Big)_4 \pmod p;$$

if $p \equiv 3 \pmod 4$, then

$$\begin{aligned}&(a^2+b^2)^{\frac{p-3}{4}}\Big(\frac{b+ai}{p}\Big)_4 \\ &\equiv (-1)^{\frac{a}{2}y+\frac{A-3}{4}}\Big(\frac{B}{A}\Big)\Big(\frac{b-ai}{A}\Big)_4\frac{y}{Ax+By} \pmod p.\end{aligned}$$

This together with (4.4) yields the result in the case.

Case 2. $2\nmid a$ and $2\mid b$. In this case, $Ap=(Ax+By)^2+(a^2+b^2)y^2 \equiv (Ax+By)^2+y^2 \equiv 1 \pmod 4$ and

$$a^2+b^2 \equiv 1+b^2 \equiv \begin{cases} 1 \pmod 8 & \text{if } 4\mid b, \\ 5 \pmod 8 & \text{if } 2\parallel b. \end{cases}$$

Thus, if $p \equiv 1 \pmod 4$, by Theorem 4.2(i) we have

$$(a^2+b^2)^{\frac{p-1}{4}} \equiv (-1)^{\frac{b}{2}y+\frac{A-1}{4}} \Big(\frac{Ax+By}{a^2+b^2}\Big)\Big(\frac{B}{A}\Big) \pmod p;$$

if $p \equiv 3 \pmod 4$, by Theorem 4.2(ii) we have

$$(a^2+b^2)^{\frac{p-3}{4}} \equiv (-1)^{\frac{b}{2}y+\frac{A-3}{4}} \Big(\frac{Ax+By}{a^2+b^2}\Big)\Big(\frac{B}{A}\Big)\frac{y}{Ax+By} \pmod p.$$

On the other hand,

$$\begin{aligned}\Big(\frac{b+ai}{p}\Big)_4&=\Big(\frac{i}{p}\Big)_4\Big(\frac{a-bi}{p}\Big)_4=i^{\frac{p^2-1}{4}}\Big(\frac{a-bi}{A}\Big)_4^{-1}\Big(\frac{a-bi}{Ap}\Big)_4\\&=(-1)^{\frac{p^2-1}{8}}\Big(\frac{a+bi}{A}\Big)_4\Big(\frac{Ap}{a-bi}\Big)_4\\&=(-1)^{\frac{p^2-1}{8}}\Big(\frac{a+bi}{A}\Big)_4\Big(\frac{(Ax+By)^2}{a-bi}\Big)_4\\&=(-1)^{\frac{p-(-1)^{(p-1)/2}}{4}}\Big(\frac{a+bi}{A}\Big)_4\Big(\frac{Ax+By}{a^2+b^2}\Big).\end{aligned}$$

Now combining the above with (4.4) gives the result in this case.

Case 3. $2\nmid ab$. In this case, $a^2+b^2\equiv 2\pmod 8$. We may choose the sign of a so that $4\mid a-b$. It is clear that $ab=a-b+b^2+(a-b)(b-1)\equiv a-b+1\pmod 8$ and thus $A(a^2+b^2)\equiv 2abA\equiv 2A(a-b+1)\equiv 2(a-b)+2A\pmod{16}$. We also have $Ap=(Ax+By)^2+(a^2+b^2)y^2\equiv 1+2y^2\equiv 2-(-1)^y\pmod 8$ and so $p\equiv A^2p\equiv (2-(-1)^y)A\pmod 8$. Hence $A\equiv(-1)^{\frac{p-1}{2}+y}\pmod 4$ and so $A^2\equiv 2(-1)^{\frac{p-1}{2}+y}A-1\pmod{16}$. We also have

$$A(a^2+b^2)y^2\equiv\begin{cases}2Ay^2\equiv 4y\pmod{16}&\text{if }2\mid y,\\ A(a^2+b^2)\equiv 2(a-b)+2A\pmod{16}&\text{if }2\nmid y.\end{cases}$$

Thus

$$\begin{aligned}&A-A^2+A(a^2+b^2)y^2\\&\equiv\begin{cases}(1-2(-1)^{(p-1)/2})A+1+4y\pmod{16}&\text{if }2\mid y,\\(3+2(-1)^{(p-1)/2})A+1+2(a-b)\pmod{16}&\text{if }2\nmid y.\end{cases}\end{aligned}$$

If $p\equiv 1\pmod 4$, by the above and Theorem 4.2(i) we have

$$(a^2+b^2)^{\frac{p-1}{4}}\equiv\begin{cases}(-1)^{\frac{p-A}{8}+\frac y2}\big(\frac BA\big)\big(\frac{Ax+By}{(a^2+b^2)/2}\big)\pmod p&\text{if }2\mid y,\\(-1)^{\frac{p+5A}{8}+\frac{a-b}{4}}\big(\frac BA\big)\big(\frac{Ax+By}{(a^2+b^2)/2}\big)\pmod p&\text{if }2\nmid y.\end{cases}$$

If $p\equiv 3\pmod 4$, by the above and Theorem 4.2(ii) we have

$$(a^2+b^2)^{\frac{p-3}{4}}\equiv\begin{cases}(-1)^{\frac{p-A}{8}-1+\frac y2}\big(\frac BA\big)\big(\frac{Ax+By}{(a^2+b^2)/2}\big)\frac{y}{Ax+By}\pmod p&\text{if }2\mid y,\\(-1)^{\frac{p+A-4}{8}+\frac{a-b}{4}}\big(\frac BA\big)\big(\frac{Ax+By}{(a^2+b^2)/2}\big)\frac{y}{Ax+By}\pmod p&\text{if }2\nmid y.\end{cases}$$

On the other hand, using [Su6, (2.8)], Lemma 4.3 and the fact $p\equiv(2-$

$(-1)^y)A \pmod 8$ we see that

$$\begin{aligned}
&\Big(\frac{b+ai}{p}\Big)_4\\
&=\Big(\frac{1+i}{p}\Big)_4\Big(\frac{\frac{a+b}{2}+\frac{a-b}{2}i}{Ap}\Big)_4\Big(\frac{\frac{a+b}{2}-\frac{a-b}{2}i}{A}\Big)_4\\
&=i^{\frac{(-1)^{\frac{p-1}{2}}p-1}{4}}(-1)^{\frac{Ap-1}{2}\cdot\frac{a-b}{4}}\Big(\frac{(Ax+By)^2+(a^2+b^2)y^2}{\frac{a+b}{2}+\frac{a-b}{2}i}\Big)_4\Big(\frac{\frac{a+b}{2}-\frac{a-b}{2}i}{A}\Big)_4\\
&=(-1)^{\frac{Ap-1}{2}\cdot\frac{a-b}{4}}i^{\frac{(-1)^{(p-1)/2}p-1}{4}}\Big(\frac{\frac{a+b}{2}-\frac{a-b}{2}i}{A}\Big)_4\Big(\frac{(Ax+By)^2}{\frac{a+b}{2}+\frac{a-b}{2}i}\Big)_4\\
&=(-1)^{\frac{a-b}{4}y}i^{\frac{(-1)^{(p-1)/2}(p-(2-(-1)^y)A)}{4}}\cdot i^{\frac{(-1)^{(p-1)/2}(2-(-1)^y)A-1}{4}}\\
&\quad\times\Big(\frac{\frac{a+b}{2}-\frac{a-b}{2}i}{A}\Big)_4\Big(\frac{Ax+By}{(a^2+b^2)/2}\Big)\\
&=(-1)^{\frac{a-b}{4}y+\frac{p-(2-(-1)^y)A}{8}}\cdot i^{\frac{(-1)^{\frac{p-1}{2}}A(2-(-1)^y)-1}{4}}\\
&\quad\times\Big(\frac{\frac{a+b}{2}-\frac{a-b}{2}i}{A}\Big)_4\Big(\frac{Ax+By}{(a^2+b^2)/2}\Big)\\
&=\begin{cases}(-1)^{\frac{p-A}{8}}i^{\frac{(-1)^{(p-1)/2}A-1}{4}}\big(\frac{\frac{a+b}{2}-\frac{a-b}{2}i}{A}\big)_4\big(\frac{Ax+By}{(a^2+b^2)/2}\big)&\text{if } 2\mid y,\\ (-1)^{\frac{a-b}{4}+\frac{p-3A}{8}}i^{\frac{-(-1)^{(p-1)/2}A-1}{4}-1}\big(\frac{\frac{a+b}{2}-\frac{a-b}{2}i}{A}\big)_4\big(\frac{Ax+By}{(a^2+b^2)/2}\big)&\text{if } 2\nmid y.\end{cases}
\end{aligned}$$

Now combining the above with (4.4) we deduce the result.

By the above the theorem is proved.

Remark 4.5 Let p be an odd prime and $a,b\in\mathbb{Z}$ with $p\nmid a(a^2+b^2)$. Then clearly

$$\Big(\frac{b+\sqrt{a^2+b^2}}{a}\Big)^{\frac{p-(\frac{-1}{p})}{2}}=\Big(\frac{\sqrt{a^2+b^2}+b}{\sqrt{a^2+b^2}-b}\Big)^{\frac{p-(\frac{-1}{p})}{4}}.$$

Set

$$f=\begin{cases}\frac{4}{(2,1+\mathrm{ord}_2 a)}&\text{if } 2\nmid b,\\ 2&\text{if } 2\nmid a \text{ and } 2\parallel b,\\ \frac{2}{(2,\mathrm{ord}_2 a)}&\text{if } 2\mid a\text{ and } 2\parallel b,\\ \frac{2}{(2,a)}&\text{if } 4\mid b\end{cases}$$

and $F=\frac{a'}{(a',b)}f$, where a' is the product of distinct odd prime divisors of a. From the above and [Su6, Theorem 4.1] we deduce the congruences for $\big(\frac{b+\sqrt{a^2+b^2}}{a}\big)^{(p-(\frac{-1}{p}))/2} \pmod p$ by expressing p in terms of binary quadratic forms of discriminant $-4F^2(a^2+b^2)$. As $4(a^2+b^2)\le 4F^2(a^2+b^2)$, Theorem 4.3 is stronger than the above result deduced from [Su6, Theorem 4.1].

If $(Ax+By)/2^{\mathrm{ord}_2(Ax+By)} \equiv 3 \pmod 4$, then

$$(A(-x)+(-B)y)/2^{\mathrm{ord}_2(A(-x)+(-B)y)} \equiv 1 \pmod 4.$$

We also have $\left(\frac{B}{A}\right) = \left(\frac{-B}{A}\right)$ for $A \equiv 1 \pmod 4$. Thus from Theorem 4.4 we deduce the following result.

Corollary 4.8. *Let $p \equiv 1 \pmod 4$ be a prime and $a, b \in \mathbb{Z}$ with $p \nmid a(a^2+b^2)$ and $a^2+b^2 \equiv 1 \pmod 8$. Suppose $p = Ax^2+2Bxy+Cy^2$ with $A, B, C, x, y \in \mathbb{Z}$, $p \nmid A$, $(A, 2(a^2+b^2)) = 1$ and $(2B)^2 - 4AC = -4(a^2+b^2)$.*
(i) *If $4 \mid a$ and $2 \nmid b$, then*

$$\left(\frac{(b+\sqrt{a^2+b^2})/2}{p}\right) = (-1)^{\frac{A-1}{4}}\left(\frac{B}{A}\right)\left(\frac{b-ai}{A}\right)_4.$$

(ii) *If $2 \nmid a$ and $4 \mid b$, then*

$$\left(\frac{b+\sqrt{a^2+b^2}}{p}\right) = (-1)^{\frac{A-1}{4}}\left(\frac{B}{A}\right)\left(\frac{a+bi}{A}\right)_4.$$

Suppose that p is a prime such that $p \equiv 1 \pmod 4$ and $p \equiv \pm1, \pm2, \pm4, \pm8 \pmod{17}$. Then p is represented by x^2+17y^2 or $9x^2+2xy+2y^2$. Taking $a = 1$ and $b = 4$ in Corollary 4.8(ii) we see that

$$\left(\frac{\varepsilon_{17}}{p}\right) = \left(\frac{4+\sqrt{17}}{p}\right) = \begin{cases} 1 & \text{if } p = x^2+17y^2, \\ \left(\frac{1+4i}{9}\right)_4 = \left(\frac{1+4i}{3}\right)_4^2 = -1 & \text{if } p = 9x^2+2xy+2y^2. \end{cases}$$

This together with Corollary 2.3 yields

$$p = x^2+17y^2 \iff \left(\frac{4+\sqrt{17}}{p}\right) = 1 \iff \left(\frac{c-4d}{17}\right) = 1, \tag{4.5}$$

where c and d are given by $p = c^2+d^2 (c, d \in \mathbb{Z})$ and $2 \mid d$.

Corollary 4.9. *Let p be an odd prime and $a, b \in \mathbb{Z}$ with $p \nmid a(a^2+b^2)$. Suppose $p = x^2+(a^2+b^2)y^2$ for some integers x and y.*
(i) *If $2 \mid a$ and $2 \nmid b$, then $\left(\frac{(b+\sqrt{a^2+b^2})/2}{p}\right) = (-1)^{\frac{a}{2}y}$.*
(ii) *If $2 \nmid a$ and $2 \mid b$, then $\left(\frac{b+\sqrt{a^2+b^2}}{p}\right) = (-1)^{\frac{b}{2}y}$.*
(iii) *If $2 \nmid ab$ and $4 \mid a-b$, then $p \equiv 2-(-1)^y \pmod 8$ and*

$$(b+\sqrt{a^2+b^2})^{\frac{p-1}{2}} \equiv \begin{cases} (-1)^{\frac{y}{2}} \pmod p & \text{if } 8 \mid p-1, \\ -\frac{y}{x}\cdot\frac{a^2+b^2-b\sqrt{a^2+b^2}}{a} \pmod p & \text{if } 8 \mid p-3 \text{ and } 4 \mid x-y. \end{cases}$$

Proof. If $a+b\equiv 1 \pmod 2$, then clearly $p=x^2+(a^2+b^2)y^2\equiv x^2+y^2\equiv 1 \pmod 4$. When $2\nmid ab$, we have $a^2+b^2\equiv 2 \pmod 8$, $2\nmid x$ and $p=x^2+(a^2+b^2)y^2\equiv 1+2y^2\equiv 2-(-1)^y \pmod 8$. Thus, if $2\nmid ab$ and $p\equiv 3 \pmod 4$, then $2\nmid xy$, $p\equiv 3 \pmod 8$ and hence $2^{\frac{p-1}{2}}\equiv -1 \pmod p$. Now taking $A=1,\ B=0$ and $C=a^2+b^2$ in Theorem 4.4 and applying the above we deduce the result.

Let p be an odd prime. From Corollary 4.9 we deduce

$$(4.6)\qquad \Big(\frac{(1+\sqrt{5})/2}{p}\Big)=(-1)^y \quad \text{for} \quad p=x^2+5y^2(x,y\in\mathbb{Z}),$$

$$(4.7)\qquad \Big(\frac{(3+\sqrt{13})/2}{p}\Big)=(-1)^y \quad \text{for} \quad p=x^2+13y^2(x,y\in\mathbb{Z}),$$

$$(4.8)\qquad \Big(\frac{6+\sqrt{37}}{p}\Big)=(-1)^y \quad \text{for} \quad p=x^2+37y^2(x,y\in\mathbb{Z}).$$

Here (4.6) is due to Vandiver [V], (4.7) and (4.8) are due to Brandler [B]. See also [Su6, Remark 6.1].

When $p\equiv 3 \pmod 8$ is a prime and $p=x^2+2y^2$ with $x\equiv y \pmod 4$, by Corollary 4.9(iii) we have $(1+\sqrt{2})^{\frac{p-1}{2}}\equiv -\frac{y}{x}(2-\sqrt{2}) \pmod p$. This result has been given in [Lem2, p. 180].

Corollary 4.10. *Let $p\equiv 1,9,11,19 \pmod{40}$ be a prime and hence $p=x^2+10y^2$ for some integers x and y. Then*

$$(3+\sqrt{10})^{\frac{p-1}{2}} \equiv \begin{cases} (-1)^{\frac{y}{2}} \pmod p & \text{if } p\equiv 1,9 \pmod{40},\\ \frac{y}{x}(10-3\sqrt{10}) \pmod p & \text{if } p\equiv 11,19 \pmod{40} \text{ and } 4\mid x-y.\end{cases}$$

Proof. Taking $a=-1$ and $b=3$ in Corollary 4.9(iii) we obtain the result.

Corollary 4.11. *Let p be an odd prime such that $p\equiv 1,3 \pmod 8$ and $\big(\frac{p}{29}\big)=1$. Then $p=x^2+58y^2$ for some $x,y\in\mathbb{Z}$ and*

$$(7+\sqrt{58})^{\frac{p-1}{2}} \equiv \begin{cases} (-1)^{\frac{y}{2}} \pmod p & \text{if } p\equiv 1 \pmod 8,\\ -\frac{y}{x}\cdot\frac{58-7\sqrt{58}}{3} \pmod p & \text{if } p\equiv 3 \pmod 8 \text{ and } 4\mid x-y.\end{cases}$$

Proof. By [SW, Table 9.1], a prime p is represented by x^2+58y^2 if and only if $\big(\frac{-2}{p}\big)=\big(\frac{p}{29}\big)=1$. Now taking $a=3$ and $b=7$ in Corollary 4.9(iii) we deduce the result.

Comparing Theorem 2.1(i) with Corollary 4.9 we have the following result.

Theorem 4.5. *Let $p \equiv 1 \pmod 4$ be a prime and $a, b \in \mathbb{Z}$ with $(a, b) = 1$ and $p \nmid a(a^2+b^2)$. Suppose $p = c^2 + d^2 = x^2 + (a^2+b^2)y^2$ with $c, d, x, y \in \mathbb{Z}$ and $2 \mid d$.*

(i) *If $2 \mid a$ and $2 \nmid b$, then $(\frac{bc+ad}{a^2+b^2}) = (-1)^{\frac{a}{2}y}$.*

(ii) *If $2 \nmid ab$, then $(-1)^{\frac{(bc+ad)^2-1}{8}}(\frac{bc+ad}{(a^2+b^2)/2}) = (-1)^{\frac{y}{2}}$.*

Suppose that $p \equiv 1 \pmod 4$ is a prime and $p = c^2 + d^2$ with $c, d \in \mathbb{Z}$ and $2 \mid d$. If $p \equiv 1, 9 \pmod{20}$, then $p = x^2 + 5y^2$ for some $x, y \in \mathbb{Z}$. Taking $a = 2$ and $b = 1$ in Theorem 4.5 we deduce $\big(\frac{c+2d}{5}\big) = (-1)^y$ and hence

$$(4.9) \qquad 2 \mid y \iff \Big(\frac{c+2d}{5}\Big) = 1 \iff \begin{cases} 5 \mid d \quad \text{and} \quad p \equiv 1 \pmod{20}, \\ 5 \mid c \quad \text{and} \quad p \equiv 9 \pmod{20}. \end{cases}$$

This result is essentially due to Lehmer [Le1]. See also [BEW, Corollary 8.3.4]. If $p \equiv \pm 1, \pm 3, \pm 4 \pmod{13}$, then $p = x^2 + 13y^2$ for some $x, y \in \mathbb{Z}$. Taking $a = 2$ and $b = 3$ in Theorem 4.5 we deduce $\big(\frac{3c+2d}{13}\big) = (-1)^y$. If $(\frac{p}{37}) = 1$, then $p = x^2 + 37y^2$ for some $x, y \in \mathbb{Z}$ (see [SW, Table 9.1]). Taking $a = 6$ and $b = 1$ in Theorem 4.5 we deduce $\big(\frac{c+6d}{37}\big) = (-1)^y$. If $p \equiv 1, 9 \pmod{40}$ and hence $p = x^2 + 40y^2$ for some $x, y \in \mathbb{Z}$, putting $a = 3$ and $b = 1$ in Theorem 4.5 we deduce $(-1)^{\frac{(c+3d)^2-1}{8}}\big(\frac{c+3d}{5}\big) = (-1)^y$.

5. Congruences for $U_{\frac{p\pm1}{2}}(b, -k^2) \pmod p$ when $p = Ax^2 + 2Bxy + Cy^2$ and $AC - B^2 = (b^2+4k^2)/(4, b^2)$.

For $n \in \mathbb{N}$ and $b, k \in \mathbb{Z}$ with $b^2 + 4k^2 \neq 0$, by (1.3) and (1.4) we have

$$(5.1) \quad U_n(b, -k^2) = \frac{1}{\sqrt{b^2+4k^2}}\Big\{\Big(\frac{b+\sqrt{b^2+4k^2}}{2}\Big)^n - \Big(\frac{b-\sqrt{b^2+4k^2}}{2}\Big)^n\Big\}$$

and

$$(5.2) \qquad V_n(b, -k^2) = \Big(\frac{b+\sqrt{b^2+4k^2}}{2}\Big)^n + \Big(\frac{b-\sqrt{b^2+4k^2}}{2}\Big)^n.$$

Theorem 5.1. *Let p be an odd prime, $b, k \in \mathbb{Z}$, $4 \nmid b^2 + k^2$ and $p \nmid k(b^2 + 4k^2)$. Let $p = Ax^2 + 2Bxy + Cy^2$ with $A, B, C, x, y \in \mathbb{Z}$, $p \nmid A$, $(A, 2(b^2+4k^2)) = 1$ and $(2B)^2 - 4AC = -\frac{4}{(4,b^2)}(b^2+4k^2)$. Assume $y/2^{\mathrm{ord}_2 y} \equiv (Ax+By)/2^{\mathrm{ord}_2(Ax+By)} \equiv 1 \pmod 4$. Let $\{U_n\}$ and $\{V_n\}$ be given by*

$$U_0 = 0,\ U_1 = 1,\ U_{n+1} = bU_n + k^2U_{n-1} \quad (n \ge 1);$$
$$V_0 = 2,\ V_1 = b,\ V_{n+1} = bV_n + k^2V_{n-1} \quad (n \ge 1).$$

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

$$p \mid U_{\frac{p-1}{2}},\ U_{\frac{p+1}{2}} \equiv \frac{1}{2}V_{\frac{p-1}{2}} \pmod p,\ V_{\frac{p+1}{2}} \equiv \frac{b}{2}V_{\frac{p-1}{2}} \pmod p$$

and

$$V_{\frac{p-1}{2}} \equiv \begin{cases} 2(-1)^{ky+\frac{A-1}{4}}\left(\frac{B}{A}\right)\left(\frac{b-2ki}{A}\right)_4 \pmod p & \textit{if } 2\nmid b, \\ 2(-1)^{\frac{y}{2}} i^{\frac{1-A}{4}}\left(\frac{B}{A}\right)\left(\frac{\frac{2k+b}{4}-\frac{2k-b}{4}i}{A}\right)_4 \pmod p & \textit{if } 8\mid b-2k \textit{ and } 2\mid y, \\ 2i^{\frac{A-3}{4}}\left(\frac{B}{A}\right)\left(\frac{\frac{2k+b}{4}-\frac{2k-b}{4}i}{A}\right)_4 \pmod p & \textit{if } 8\mid b-2k \textit{ and } 2\nmid y, \\ 2(-1)^{\frac{A-1}{4}+\frac{b}{4}y}\left(\frac{B}{A}\right)\left(\frac{k+\frac{b}{2}i}{A}\right)_4 \pmod p & \textit{if } 4\mid b. \end{cases}$$

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

$$p \mid V_{\frac{p+1}{2}},\ U_{\frac{p-1}{2}} \equiv -\frac{b}{b^2+4k^2}V_{\frac{p-1}{2}} \pmod p,\ U_{\frac{p+1}{2}} \equiv \frac{2k^2}{b^2+4k^2}V_{\frac{p-1}{2}} \pmod p$$

and

$$V_{\frac{p-1}{2}} \equiv \begin{cases} (-1)^{ky+\frac{A-3}{4}}\left(\frac{B}{A}\right)\left(\frac{b-2ki}{A}\right)_4 i^{\frac{(b^2+4k^2)y}{k(Ax+By)}} \pmod p \\ \qquad \textit{if } 2\nmid b, \\ (-1)^{\frac{y}{2}} i^{\frac{A-3}{4}}\left(\frac{B}{A}\right)\left(\frac{\frac{2k+b}{4}-\frac{2k-b}{4}i}{A}\right)_4^{\frac{(b^2+4k^2)y}{2k(Ax+By)}} \pmod p \\ \qquad \textit{if } 8\mid b-2k \textit{ and } 2\mid y, \\ -i^{\frac{1-A}{4}}\left(\frac{B}{A}\right)\left(\frac{\frac{2k+b}{4}-\frac{2k-b}{4}i}{A}\right)_4^{\frac{(b^2+4k^2)y}{2k(Ax+By)}} \pmod p \\ \qquad \textit{if } 8\mid b-2k \textit{ and } 2\nmid y, \\ (-1)^{\frac{A-3}{4}+\frac{b}{4}y}\left(\frac{B}{A}\right)\left(\frac{k+\frac{b}{2}i}{A}\right)_4 i^{\frac{(b^2+4k^2)y}{2k(Ax+By)}} \pmod p \\ \qquad \textit{if } 4\mid b \end{cases}$$

Proof. We first determine $\left(\frac{b\pm\sqrt{b^2+4k^2}}{2}\right)^{\frac{p-1}{2}} \pmod p$ by considering the following three cases.

Case 1. $2\nmid b$. Taking $a=2k$ in Theorem 4.4 we see that

$$\begin{aligned} &\left(\frac{b\pm\sqrt{b^2+4k^2}}{2}\right)^{\frac{p-1}{2}} \\ &\equiv \begin{cases} (-1)^{ky+\frac{A-1}{4}}\left(\frac{B}{A}\right)\left(\frac{b-2ki}{A}\right)_4 \pmod p & \text{if } p\equiv 1 \pmod 4, \\ (-1)^{ky+\frac{A-3}{4}}\left(\frac{B}{A}\right)\left(\frac{b-2ki}{A}\right)_4 i^{\frac{y}{Ax+By}\cdot\frac{b^2+4k^2\mp b\sqrt{b^2+4k^2}}{2k}} \pmod p \\ & \text{if } p\equiv 3 \pmod 4, \end{cases} \end{aligned}$$

Case 2. $2\parallel b$. In this case, $b/2$ and k are odd. We choose the sign of k so that $k\equiv b/2 \pmod 4$. As $Ap=(Ax+By)^2+((\frac{b}{2})^2+k^2)y^2\equiv(Ax+By)^2+2y^2\equiv 1+2y^2\equiv 2-(-1)^y \pmod 8$ we have $p\equiv A^2p\equiv(2-(-1)^y)A \pmod 8$. Thus

$$2^{\frac{p-1}{2}} \equiv (-1)^{\frac{p-(\frac{-1}{p})}{4}} = (-1)^{\frac{(2-(-1)^y)A-(\frac{-1}{p})}{4}} \pmod p.$$

Now applying the above and replacing a, b by $k, b/2$ in Theorem 4.4 we obtain

$$\begin{aligned}
&(-1)^{\frac{(2-(-1)^y)A-(\frac{-1}{p})}{4}}\Big(\frac{b\pm\sqrt{b^2+4k^2}}{2}\Big)^{\frac{p-1}{2}}\\
&\equiv\Big(\frac{\frac b2\pm\sqrt{(\frac b2)^2+k^2}}{2}\Big)^{\frac{p-1}{2}}\\
&\equiv\begin{cases}
(-1)^{\frac y2}i^{\frac{A-1}{4}}\big(\frac BA\big)\Big(\frac{\frac{2k+b}{4}-\frac{2k-b}{4}i}{A}\Big)_4 \pmod p & \text{if } 4\mid p-1 \text{ and } 2\mid y,\\
i^{\frac{3-A}{4}}\big(\frac BA\big)\Big(\frac{\frac{2k+b}{4}-\frac{2k-b}{4}i}{A}\Big)_4 \pmod p & \text{if } 4\mid p-1 \text{ and } 2\nmid y,\\
(-1)^{\frac y2+1}i^{\frac{3-A}{4}}\big(\frac BA\big)\Big(\frac{\frac{2k+b}{4}-\frac{2k-b}{4}i}{A}\Big)_4^{\frac{y}{Ax+By}}\cdot\frac{(\frac b2)^2+k^2\mp\frac b2\sqrt{(\frac b2)^2+k^2}}{k} \pmod p\\
\qquad & \text{if } 4\mid p-3 \text{ and } 2\mid y,\\
i^{\frac{A-1}{4}}\big(\frac BA\big)\Big(\frac{\frac{2k+b}{4}-\frac{2k-b}{4}i}{A}\Big)_4^{\frac{y}{Ax+By}}\cdot\frac{(\frac b2)^2+k^2\mp\frac b2\sqrt{(\frac b2)^2+k^2}}{k} \pmod p\\
\qquad & \text{if } 4\mid p-3 \text{ and } 2\nmid y.
\end{cases}
\end{aligned}$$

Case 3. $4\mid b$. In this case, k is odd and $b/2$ is even. Substituting a, b by $k, b/2$ in Theorem 4.4 we see that

$$\begin{aligned}
&(-1)^{\frac{p-(\frac{-1}{p})}{4}}\Big(\frac{b\pm\sqrt{b^2+4k^2}}{2}\Big)^{\frac{p-1}{2}}\\
&\equiv\Big(\frac{\frac b2\pm\sqrt{(\frac b2)^2+k^2}}{2}\Big)^{\frac{p-1}{2}}\\
&\equiv\begin{cases}
(-1)^{\frac{p-A}{4}+\frac b4 y}\big(\frac BA\big)\Big(\frac{k+\frac b2 i}{A}\Big)_4 \pmod p & \text{if } p\equiv 1 \pmod 4,\\
(-1)^{\frac{p-A}{4}+1+\frac b4 y}\big(\frac BA\big)\Big(\frac{k+\frac b2 i}{A}\Big)_4 i^{\frac{y}{Ax+By}}\cdot\frac{(\frac b2)^2+k^2\mp\frac b2\sqrt{(\frac b2)^2+k^2}}{k} \pmod p\\
\qquad & \text{if } p\equiv 3 \pmod 4.
\end{cases}
\end{aligned}$$

By (3.1) we have

$$U_{\frac{p+1}{2}}=\frac12\big(bU_{\frac{p-1}{2}}+V_{\frac{p-1}{2}}\big)\quad\text{and}\quad V_{\frac{p+1}{2}}=\frac12\big((b^2+4k^2)U_{\frac{p-1}{2}}+bV_{\frac{p-1}{2}}\big).$$

If $p\equiv 1 \pmod 4$, by the above congruences for $\big(\frac{b\pm\sqrt{b^2+4k^2}}{2}\big)^{\frac{p-1}{2}} \pmod p$ and (5.1)-(5.2) we deduce $p\mid U_{\frac{p-1}{2}}$ and the congruence for $V_{\frac{p-1}{2}} \pmod p$. As $p\mid U_{\frac{p-1}{2}}$, we have $U_{\frac{p+1}{2}}\equiv\frac12 V_{\frac{p-1}{2}} \pmod p$ and $V_{\frac{p+1}{2}}\equiv\frac b2 V_{\frac{p-1}{2}} \pmod p$. If $p\equiv 3 \pmod 4$, as

$$\frac{b^2+4k^2\mp b\sqrt{b^2+4k^2}}{2k}\cdot\frac{b\pm\sqrt{b^2+4k^2}}{2}=\pm k\sqrt{b^2+4k^2},$$

by the above congruences for $\left(\frac{b\pm\sqrt{b^2+4k^2}}{2}\right)^{\frac{p-1}{2}} \pmod p$ and (5.2) we deduce $p \mid V_{\frac{p+1}{2}}$ and the congruence for $V_{\frac{p-1}{2}} \pmod p$. Since $p \mid V_{\frac{p+1}{2}}$ we have $U_{\frac{p-1}{2}} \equiv -\frac{b}{b^2+4k^2}V_{\frac{p-1}{2}} \pmod p$ and

$$U_{\frac{p+1}{2}} \equiv \frac{1}{2}\Big(-\frac{b^2}{b^2+4k^2}V_{\frac{p-1}{2}}+V_{\frac{p-1}{2}}\Big)=\frac{2k^2}{b^2+4k^2}V_{\frac{p-1}{2}} \pmod p.$$

This completes the proof.

Corollary 5.1. *Let p be an odd prime and let $\{U_n\}$ be given by $U_0=0,\ U_1=1$ and $U_{n+1}=3U_n+U_{n-1}$ $(n\ge 1)$.*

(i) *If $p\equiv 1 \pmod 4$, $p\equiv \pm1,\pm3,\pm4 \pmod{13}$ and hence $p=x^2+13y^2$ for some $x,y\in\mathbb{Z}$, then $p\mid U_{\frac{p-1}{2}}$ and $U_{\frac{p+1}{2}}\equiv(-1)^y \pmod p$.*

(ii) *If $p\equiv 3 \pmod 4$, $p\equiv\pm2,\pm5,\pm6 \pmod{13}$, $p\ne 7$ and hence $p=7x^2+2xy+2y^2$ for some $x,y\in\mathbb{Z}$, then*

$$U_{\frac{p-1}{2}}\equiv(-1)^{y+1}\frac{3y}{7x+y} \pmod p \quad \text{and} \quad U_{\frac{p+1}{2}}\equiv(-1)^y\frac{2y}{7x+y} \pmod p,$$

where x and y are chosen so that $y/2^{\mathrm{ord}_2 y}\equiv(7x+y)/2^{\mathrm{ord}_2(7x+y)}\equiv 1 \pmod 4$.

Proof. If $p\equiv 1 \pmod 4$ and $p\equiv\pm1,\pm3,\pm4 \pmod{13}$, by [SW, Table 9.1] we have $p=x^2+13y^2$ for some $x,y\in\mathbb{Z}$. Now putting $A=1,\ B=0,\ C=13,\ b=3$ and $k=1$ in Theorem 5.1(i) we see that $p\mid U_{\frac{p-1}{2}}$ and $U_{\frac{p+1}{2}}\equiv(-1)^y \pmod p$. If $p\equiv 3 \pmod 4$ and $p\equiv\pm2,\pm5,\pm6 \pmod{13}$, by [SW, Table 9.1] we have $p=7x^2\pm 2xy+2y^2$ for some $x,y\in\mathbb{Z}$. We choose the signs of x and y so that $y/2^{\mathrm{ord}_2 y}\equiv(7x\pm y)/2^{\mathrm{ord}_2(7x\pm y)}\equiv 1 \pmod 4$. Putting $A=7,\ B=1,\ C=2,\ b=3$ and $k=1$ in Theorem 5.1(ii) we see that

$$U_{\frac{p-1}{2}}\equiv-\frac{3}{13}(-1)^{y+1}\Big(\frac{\pm1}{7}\Big)\Big(\frac{3-2i}{7}\Big)_4 i\frac{13y}{7x\pm y}=(-1)^{y+1}\frac{3y}{y\pm 7x} \pmod p$$

and

$$U_{\frac{p+1}{2}}\equiv\frac{2}{13}(-1)^{y+1}\Big(\frac{\pm1}{7}\Big)\Big(\frac{3-2i}{7}\Big)_4 i\frac{13y}{7x\pm y}=(-1)^{y}\frac{2y}{y\pm 7x} \pmod p$$

This completes the proof.

Corollary 5.2. *Let $p\equiv 1 \pmod 4$ be a prime, $b,k\in\mathbb{Z}$, $2\parallel b$, $2\nmid k$ and $p\nmid k(b^2+4k^2)$. Suppose $p=\frac{b^2+4k^2}{8}x^2+2y^2$ for some $x,y\in\mathbb{Z}$. Then*

$$p\mid U_{\frac{p-1}{2}}(b,-k^2),\quad U_{\frac{p+1}{2}}(b,-k^2)\equiv\frac{1}{2}V_{\frac{p-1}{2}}(b,-k^2)\equiv(-1)^{\frac{(\frac{b}{2})^2-1}{8}+\frac{y}{2}} \pmod p$$

and

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

Proof. We choose the signs of k and x so that $k \equiv b/2 \pmod 4$ and $x \equiv 1 \pmod 4$. Set $c = (b^2+4k^2)/8$. Then $c \equiv 1 \pmod 4$ and hence $p = cx^2 + 2y^2 \equiv 2y+1 \pmod 4$. As $p \equiv 1 \pmod 4$ we have $2 \mid y$. Clearly $p = cx^2+2y^2 = (c+2)x^2 - 4x(x-y) + 2(x-y)^2$, $(c+2)x \pm 2(x-y) \equiv cx \equiv 1 \pmod 4$ and $(-1)^{\frac{y}{2}}(x-y) \equiv 1 \pmod 4$. We also have $(c+2, 2(b^2+4k^2)) = 1$ and $2 \nmid x-y$. If $p \mid c+2$, then $2(x^2-y^2) = (c+2)x^2 - p \equiv 0 \pmod p$. As $0 \le x^2, y^2 < p$ we deduce $x^2 = y^2$. But $2 \nmid x$ and $2 \mid y$. Thus $x^2 \ne y^2$ and so $p \nmid c+2$. Now putting $A = c+2$, $B = 2(-1)^{\frac{y}{2}+1}$, $C = 2$ and substituting y by $(-1)^{\frac{y}{2}}(x-y)$ in Theorem 5.1(i) and then applying [Su6, (2.7) and (2.8)] we obtain

$$\begin{aligned}\frac{1}{2}V_{\frac{p-1}{2}}(b,-k^2) &\equiv i^{\frac{(c+2)-3}{4}}\Big(\frac{2(-1)^{\frac{y}{2}+1}}{c+2}\Big)\Big(\frac{\frac{2k+b}{4}-\frac{2k-b}{4}i}{c+2}\Big)_4\\ &= i^{\frac{c-1}{4}}(-1)^{\frac{c+3}{4}}\cdot(-1)^{\frac{y}{2}+1}\cdot(-1)^{\frac{c+1}{2}\cdot\frac{2k-b}{8}}\Big(\frac{c+2}{\frac{2k+b}{4}-\frac{2k-b}{4}i}\Big)_4\\ &= (-1)^{\frac{2k-b}{8}+\frac{y}{2}+\frac{c-1}{4}} i^{\frac{c-1}{4}}\Big(\frac{2}{\frac{2k+b}{4}-\frac{2k-b}{4}i}\Big)_4\\ &= (-1)^{\frac{2k-b}{8}+\frac{y}{2}+\frac{c-1}{4}} i^{\frac{c-1}{4}}\cdot i^{(-1)^{\frac{b-2}{4}}\frac{2k-b}{8}} \pmod p\end{aligned}$$

Set $t = (2k-b)/8$. Then $\frac{b-2}{4} = \frac{k-1}{2} - 2t$ and

$$c = \frac{b^2+4k^2}{8} = \frac{(2k-b)^2+4(2k-8t)k}{8} = 8t^2 + k^2 - 4kt.$$

Thus

$$\begin{aligned}&(-1)^{\frac{2k-b}{8}} i^{\frac{c-1}{4}}\cdot i^{(-1)^{\frac{b-2}{4}}\frac{2k-b}{8}}\\ &= (-1)^t i^{\frac{8t^2-4kt+k^2-1}{4}}\cdot i^{(-1)^{\frac{b-2}{4}}t} = (-1)^t\cdot(-1)^{t^2+\frac{k^2-1}{8}} i^{-kt}\cdot i^{(-1)^{\frac{k-1}{2}}t}\\ &= (-1)^{\frac{k^2-1}{8}} i^{((-1)^{\frac{k-1}{2}}-k)t} = (-1)^{\frac{k^2-1}{8}}.\end{aligned}$$

Hence

$$\begin{aligned}\frac{1}{2}V_{\frac{p-1}{2}}(b,-k^2) &\equiv (-1)^{\frac{y}{2}+\frac{c-1}{4}}\cdot(-1)^{\frac{k^2-1}{8}} = (-1)^{\frac{y}{2}+\frac{(\frac{b}{2})^2+k^2-2}{8}+\frac{k^2-1}{8}}\\ &= (-1)^{\frac{(\frac{b}{2})^2-1}{8}+\frac{y}{2}} \pmod p.\end{aligned}$$

By Theorem 5.1(i), $p \mid U_{\frac{p-1}{2}}(b,-k^2)$, $U_{\frac{p+1}{2}}(b,-k^2) \equiv \frac{1}{2}V_{\frac{p-1}{2}}(b,-k^2) \pmod p$ and $V_{\frac{p+1}{2}}(b,-k^2) \equiv \frac{b}{2}V_{\frac{p-1}{2}}(b,-k^2) \pmod p$. So the corollary is proved.

From (3.2) and Theorem 5.1 we deduce the following result.

Theorem 5.2. *Let $p \equiv 1 \pmod 4$ be a prime, $b,k \in \mathbb{Z}$, $4 \nmid b^2+k^2$ and $p \nmid k(b^2+4k^2)$. Suppose $p = Ax^2+2Bxy+Cy^2$ with $A,B,C,x,y \in \mathbb{Z}$, $p \nmid A$, $(A, 2(b^2+4k^2)) = 1$ and $(2B)^2-4AC = -\frac{4}{(4,b^2)}(b^2+4k^2)$. Assume $y/2^{\mathrm{ord}_2 y} \equiv (Ax+By)/2^{\mathrm{ord}_2(Ax+By)} \equiv 1 \pmod 4$. Then $p \mid U_{\frac{p-1}{4}}(b,-k^2)$ if and only if*

$$\Big(\frac{k}{p}\Big) = \begin{cases} (-1)^{\frac{(Ax+By)y}{2}}\big(\frac{B}{A}\big)\big(\frac{b-2ki}{A}\big)_4 & \text{if } 2 \nmid b, \\ (-1)^{\frac{y}{2}} i^{\frac{A-1}{4}}\big(\frac{B}{A}\big)\big(\frac{\frac{2k+b}{4}-\frac{2k-b}{4}i}{A}\big)_4 & \text{if } 8 \mid b-2k \text{ and } 4 \mid A-1, \\ i^{\frac{3-A}{4}}\big(\frac{B}{A}\big)\big(\frac{\frac{2k+b}{4}-\frac{2k-b}{4}i}{A}\big)_4 & \text{if } 8 \mid b-2k \text{ and } 4 \mid A-3, \\ (-1)^{\frac{(Ax+By)y}{2}}\big(\frac{B}{A}\big)\big(\frac{k+\frac{b}{2}i}{A}\big)_4 & \text{if } 4 \mid b. \end{cases}$$

Proof. If $2 \parallel b$, then $(\frac{b}{2})^2+k^2 \equiv 2 \pmod 8$ and thus $Ap = (Ax+By)^2 + ((\frac{b}{2})^2+k^2)y^2 \equiv 1+2y^2 \equiv 2-(-1)^y \pmod 8$. Thus $A \equiv Ap \equiv 2-(-1)^y \equiv (-1)^y \pmod 4$ and

$$(-1)^{\frac{p-1}{4}} = (-1)^{\frac{Ap-A}{4}} = (-1)^{\frac{2-(-1)^y-A}{4}} = \begin{cases} (-1)^{\frac{A-1}{4}} & \text{if } 4 \mid A-1, \\ (-1)^{\frac{A-3}{4}} & \text{if } 4 \mid A-3. \end{cases}$$

If $4 \nmid b-2$, then $(b^2+4k^2)/(4,b^2)$ is odd. Hence

$$\begin{aligned}(-1)^{\frac{p-1}{4}} &= (-1)^{\frac{Ap-A}{4}} = (-1)^{((Ax+By)^2+\frac{b^2+4k^2}{(4,b^2)}y^2-A)/4} \\ &= \begin{cases} (-1)^{\frac{y^2(b^2+4k^2)/(4,b^2)-A+1}{4}} = (-1)^{\frac{y}{2}+\frac{A-1}{4}} & \text{if } 2 \mid y, \\ (-1)^{\frac{Ax+By}{2}+\frac{1-A}{4}+k} & \text{if } 2 \nmid by, \\ (-1)^{\frac{Ax+By}{2}+\frac{1-A}{4}+\frac{b}{4}} & \text{if } 4 \mid b \text{ and } 2 \nmid y. \end{cases}\end{aligned}$$

From (3.2) we know that $p \mid U_{\frac{p-1}{4}}$ if and only if $V_{\frac{p-1}{2}} \equiv 2(-1)^{\frac{p-1}{4}}\big(\frac{k}{p}\big) \pmod p$. Thus applying the above and Theorem 5.1(i) we deduce the result.

Putting $A=1$, $B=0$ and $C=(b^2+4k^2)/(4,b^2)$ in Theorem 5.2 we have:

Corollary 5.3. *Let $p \equiv 1 \pmod 4$ be a prime, $b,k \in \mathbb{Z}$, $4 \nmid b^2+k^2$ and $p \nmid k(b^2+4k^2)$. Suppose $p = x^2+\frac{b^2+4k^2}{(4,b^2)}y^2$ for some $x,y \in \mathbb{Z}$. Then*

$$p \mid U_{\frac{p-1}{4}}(b,-k^2) \iff \Big(\frac{k}{p}\Big) = (-1)^{\frac{xy}{2}}.$$

Remark 5.1 When $k=1$ and $2 \nmid b$, Corollary 5.3 has been given in [Su5, Theorem 5.3]. See also [Su6, Corollary 7.1].

Theorem 5.3. *Let $p \equiv 1 \pmod 4$ be a prime, $b, k \in \mathbb{Z}$, $2 \parallel b$, $2 \nmid k$ and $p \nmid k(b^2+4k^2)$. Suppose $p = \frac{b^2+4k^2}{8}x^2 + 2y^2$ for some $x, y \in \mathbb{Z}$. Then $p \mid U_{\frac{p-1}{4}}(b, -k^2)$ if and only if $(-1)^{\frac{k^2-1}{8}}\left(\frac{k}{p}\right) = (-1)^{\frac{y}{2}}$.*

Proof. As $p \equiv 1 \pmod 4$ we have $2 \nmid x$ and $2 \mid y$. Thus $p = \frac{b^2+4k^2}{8}x^2 + 2y^2 \equiv \frac{1}{2}((\frac{b}{2})^2 + k^2) \pmod 8$ and hence $\left(\frac{2}{p}\right) = (-1)^{\frac{p-1}{4}} = (-1)^{\frac{(\frac{b}{2})^2+k^2-2}{8}}$. Therefore, by (3.2) and Corollary 5.2 we have

$$\begin{aligned} p \mid U_{\frac{p-1}{4}}(b, -k^2) &\iff V_{\frac{p-1}{2}}(b, -k^2) \equiv 2\Big(\frac{2k}{p}\Big) \pmod p \\ &\iff (-1)^{\frac{(\frac{b}{2})^2-1}{8}+\frac{y}{2}} = \Big(\frac{2k}{p}\Big) \\ &\iff (-1)^{\frac{(\frac{b}{2})^2-1}{8}+\frac{y}{2}} = (-1)^{\frac{(\frac{b}{2})^2+k^2-2}{8}}\Big(\frac{k}{p}\Big) \\ &\iff (-1)^{\frac{y}{2}} = (-1)^{\frac{k^2-1}{8}}\Big(\frac{k}{p}\Big). \end{aligned}$$

This proves the theorem.

Corollary 5.4. *Let $b \in \{2, 14\}$. Let $p \neq 2b+1$ be a prime of the form $4n+1$. Then $p \mid U_{\frac{p-1}{4}}(b, -9)$ if and only if $p = x^2 + 8(2b+1)y^2$ with $x, y \in \mathbb{Z}$ and $(-1)^y = \left(\frac{p}{3}\right)$, or $p = (2b+1)x^2 + 8y^2$ with $x, y \in \mathbb{Z}$ and $(-1)^y = -\left(\frac{p}{3}\right)$.*

Proof. From Remark 3.2 we know that $p \nmid U_{\frac{p-1}{4}}(b, -9)$ when $(\frac{4b+2}{p}) = -1$. If $p = x^2+8(2b+1)y^2$ or $(2b+1)x^2+8y^2$, then clearly $(\frac{4b+2}{p}) = (\frac{-2(2b+1)}{p}) = 1$. So the result holds when $(\frac{4b+2}{p}) = -1$. Now assume $(\frac{4b+2}{p}) = (\frac{-4b-2}{p}) = 1$. From [SW, Table 9.1] we know that $p = x^2 + (4b+2)y^2$ or $(2b+1)x^2 + 2y^2$ according as $(\frac{-2}{p}) = (\frac{p}{2b+1}) = 1$ or $(\frac{-2}{p}) = (\frac{p}{2b+1}) = -1$. If $p \equiv 1 \pmod 8$ and $(\frac{p}{2b+1}) = 1$, then $p = x^2+(4b+2)y^2$ with $2 \mid y$. Taking $k = 3$ in Corollary 5.3 we see that

$$p \mid U_{\frac{p-1}{4}}(b, -9) \iff \Big(\frac{3}{p}\Big) = (-1)^{\frac{xy}{2}} \iff \Big(\frac{p}{3}\Big) = (-1)^{\frac{y}{2}}.$$

If $p \equiv 5 \pmod 8$ and $(\frac{p}{2b+1}) = -1$, then $p = (2b+1)x^2 + 2y^2$ with $2 \mid y$. Taking $k = 3$ in Theorem 5.3 we obtain

$$p \mid U_{\frac{p-1}{4}}(b, -9) \iff (-1)^{\frac{3^2-1}{8}}\Big(\frac{3}{p}\Big) = (-1)^{\frac{y}{2}} \iff (-1)^{\frac{y}{2}} = -\Big(\frac{p}{3}\Big).$$

The proof is now complete.

Theorem 5.4. *Let p be an odd prime.*

(i) *If $p \equiv 1, 9, 11, 19 \pmod{40}$ and hence $p = x^2 + 10y^2$ for some integers x and y, then*

$$U_{\frac{p-1}{2}}(6, -1) \equiv \begin{cases} 0 \pmod p & \text{if } p \equiv 1, 9 \pmod{40}, \\ -\frac{3y}{x} \pmod p & \text{if } p \equiv 11, 19 \pmod{40} \text{ and } 4 \mid x - y \end{cases}$$

and

$$U_{\frac{p+1}{2}}(6, -1) \equiv \begin{cases} (-1)^{\frac{y}{2}} \pmod p & \text{if } p \equiv 1, 9 \pmod{40}, \\ \frac{y}{x} \pmod p & \text{if } p \equiv 11, 19 \pmod{40} \text{ and } 4 \mid x - y. \end{cases}$$

(ii) *If $p \equiv 13, 37 \pmod{40}$ and hence $p = 5x^2 + 2y^2$ for some integers x and y, then $p \mid U_{\frac{p-1}{2}}(6, -1)$ and $U_{\frac{p+1}{2}}(6, -1) \equiv (-1)^{\frac{y}{2}+1} \pmod p$.*

Proof. From (1.3) and Corollary 4.10 we deduce (i). Putting $b = 6$ and $k = 1$ in Corollary 5.2 we deduce (ii). So the theorem is proved.

Theorem 5.5. *Let p be an odd prime.*

(i) *If $(\frac{-2}{p}) = (\frac{p}{29}) = 1$ and hence $p = x^2 + 58y^2$ for some integers x and y, then*

$$U_{\frac{p-1}{2}}(14, -9) \equiv \begin{cases} 0 \pmod p & \text{if } p \equiv 1 \pmod 8, \\ \frac{7y}{3x} \pmod p & \text{if } p \equiv 3 \pmod 8 \text{ and } 4 \mid x - y \end{cases}$$

and

$$U_{\frac{p+1}{2}}(14, -9) \equiv \begin{cases} (-1)^{\frac{y}{2}} \pmod p & \text{if } p \equiv 1 \pmod 8, \\ -\frac{3y}{x} \pmod p & \text{if } p \equiv 3 \pmod 8 \text{ and } 4 \mid x - y. \end{cases}$$

(ii) *If $p \equiv 5 \pmod 8$, $(\frac{p}{29}) = -1$ and hence $p = 29x^2 + 2y^2$ for some integers x and y, then $p \mid U_{\frac{p-1}{2}}(14, -9)$ and $U_{\frac{p+1}{2}}(14, -9) \equiv (-1)^{\frac{y}{2}} \pmod p$.*

Proof. From (1.3) and Corollary 4.11 we deduce (i). Putting $b = 14$ and $k = 3$ in Corollary 5.2 we deduce (ii). So the theorem is proved.

References

[AR] A. Aigner and H. Reichardt, *Stufenreihen im Potenzrestcharakter*, J. Reine Angew. Math. **184** (1942), 158-160.

[BC] P. Barrucand and H. Cohn, *Note on primes of type $x^2 + 32y^2$, class number, and residuacity*, J. Reine Angew. Math. **238** (1969), 67-70.

[BEW] B.C. Berndt, R.J. Evans and K.S. Williams, *Gauss and Jacobi Sums*, Wiley, New York, 1998, p. 256.

[B] J. Brandler, *Residuacity properties of real quadratic units*, J. Number Theory **5** (1973), 271-287.

[Bro1] E. Brown, *A theorem on biquadratic reciprocity*, Proc. Amer. Math. Soc. **30** (1971), 220-222.

[Bro2] E. Brown, *Quadratic forms and biquadratic reciprocity*, J. Reine Angew. Math. **253** (1972), 214-220.

[BLW] D.A. Buell, P.A. Leonard and K.S. Williams, *Note on the quadratic character of a quadratic unit*, Pacific J. Math. **92** (1981), 35-38.

[Bu] K. Burde, *Ein rationales biquadratisches Reziprozitätsgesetz*, J. Reine Angew. Math. **235** (1969), 175-184.

[D] H. Dörrie, *Das quadratische Reciprocitätsgesetz in quadratischen Zahlkörpern mit der Classenzahl* 1, Diss. Göttingen, 1898.

[E1] R.J. Evans, *Rational reciprocity laws*, Acta Arith. **39** (1981), 281-294.

[E2] R.J. Evans, *Residuacity of primes*, Rocky Mountain J. Math. **19** (1989), 1069-1081.

[FK] Y. Furuta and P. Kaplan, *On quadratic and quartic characters of quadratic units*, Sci. Rep. Kanazawa Univ. **26** (1981), 27-30.

[K] K. Kramer, *Residue properties of certain quadratic units*, J. Number Theory **21** (1985), 204-213.

[HW] R.H. Hudson and K.S. Williams, *Some new residuacity criteria*, Pacific J. Math. **91** (1980), 135-143.

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

[KWY] P. Kaplan, K.S. Williams and Y. Yamamoto, *An application of dihedral fields to representations of primes by binary quadratic forms*, Acta Arith. **44** (1984), 407-413.

[L] D.H. Lehmer, *An extended theory of Lucas' functions*, Ann. Math. **31** (1930), 419-448.

[Le1] E. Lehmer, *On the quadratic character of the Fibonacci root*, Fibonacci Quart. **4** (1966), 135-138.

[Le2] E. Lehmer, *On the quadratic character of some quadratic surds*, J. Reine Angew. Math. **250** (1971), 42-48.

[Le3] E. Lehmer, *On some special quartic reciprocity laws*, Acta Arith. **21** (1972), 367-377.

[Le4] E. Lehmer, *On the quartic character of quadratic units*, J. Reine Angew. Math. **268/269** (1974), 294-301.

[Le5] E. Lehmer, *Rational reciprocity laws*, Amer. Math. Monthly **85** (1978), 467-472.

[Lem1] F. Lemmermeyer, *Rational quartic reciprocity*, Acta Arith. **67** (1994), 387-390.

[Lem2] F. Lemmermeyer, *Reciprocity Laws: From Euler to Eisenstein*, Springer, Berlin, 2000.

[LW1] P.A. Leonard and K.S. Williams, *The quadratic and quartic character of certain quadratic units I*, Pacific J. Math. **71** (1977), 101-106.

[LW2] P.A. Leonard and K.S. Williams, *The quadratic and quartic character of certain quadratic units II*, Rocky Mountain J. Math. **9** (1979), 683-691.

[LW3] P.A. Leonard and K.S. Williams, *A representation problem involving binary quadratic forms*, Archiv der Math. **36** (1981), 53-56.

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

[Sc] T.H. Schönemann, *Theorie der symmetrischen Functionen der Wurzeln einer Gleichung. Allgemeine Sätze über Congruenzen nebst einigen Anwendungen derselben*, J. Reine Angew. Math. **19** (1839), 289-308.

[Su1] Z.H. Sun, *Notes on quartic residue symbol and rational reciprocity laws*, J. Nanjing Univ. Math. Biquarterly **9** (1992), 92-101.

[Su2] Z.H. Sun, *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.

[Su3] Z.H. Sun, *On the theory of cubic residues and nonresidues*, Acta Arith. **84** (1998), 291-335.

[Su4] Z.H. Sun, *Supplements to the theory of quartic residues*, Acta Arith. **97** (2001), 361-377.

[Su5] Z.H. Sun, *Values of Lucas sequences modulo primes*, Rocky Mountain J. Math. **33** (2003), 1123-1145.

[Su6] Z.H. Sun, *Quartic residues and binary quadratic forms*, J. Number Theory **113** (2005), 10-52.

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

[SW] Z.H. Sun and K.S. Williams, *On the number of representations of* n *by* $ax^2+bxy+cy^2$, Acta Arith. **122** (2006), 101-171.

[V] H.S. Vandiver, *Problem 152*, Amer. Math. Monthly **15** (1908), 46, 235.

[W] H.C. Williams, *The quadratic character of a certain quadratic surd*, Utilitas Math. **5** (1974), 49-55.

[Wi1] K.S. Williams, *Note on a result of Barrucand and Cohn*, J. Reine Angew. Math. **285** (1976), 218-220.

[Wi2] K.S. Williams, *A rational octic reciprocity law*, Pacific J. Math. **63** (1976), 563-570.

[Wi3] K.S. Williams, *On Scholz's reciprocity law*, Proc. Amer. Math. Soc. **64** (1977), 45-46.

[Wi4] K.S. Williams, *On the evaluation of* $(\varepsilon_{q_1q_2}/p)$, Rocky Mountain J. Math. **10** (1980), 559-573.

[Wi5] K.S. Williams, *On Yamamoto's reciprocity law*, Proc. Amer. Math. Soc. **111** (1991), 607-609.

[WHF] K.S. Williams, K. Hardy and C. Friesen, *On the evaluation of the Legendre symbol* $\frac{A+B\sqrt{m}}{p}$, Acta Arith. **45** (1985), 255-272.