ROCKY MOUNTAIN
JOURNAL OF MATHEMATICS
Volume 33, Number 3, Fall 2003

VALUES OF LUCAS SEQUENCES MODULO PRIMES

ZHI-HONG SUN

ABSTRACT. Let p be an odd prime, and a, b be two integers. It is the purpose of the paper to determine the values of $u_{(p\pm 1)/2}(a,b) \pmod p$, where $\{u_n(a,b)\}$ is the Lucas sequence given by $u_0(a,b)=0$, $u_1(a,b)=1$ and $u_{n+1}(a,b) = bu_n(a,b) - au_{n-1}(a,b)$ $(n \geq 1)$. In the case $a=-c^2$, a reciprocity law is established. As applications we obtain the criteria for $p \mid u_{(p-1)/4}(a,b)$ (if $p \equiv 1 \pmod 4$) and for $k \in Q_0(p)$ and $k \in Q_1(p)$, where $Q_0(p)$ and $Q_1(p)$ are defined as in [**10**].

1. Introduction. Let a and b be two real numbers. The Lucas sequences $\{u_n(a,b)\}$ and $\{v_n(a,b)\}$ are defined as follows:

$$
\begin{gathered}
u_0(a,b)=0, \quad u_1(a,b)=1, \\
u_{n+1}(a,b) = bu_n(a,b) - au_{n-1}(a,b), \quad n \geq 1;
\end{gathered} \tag{1.1}
$$

$$
\begin{gathered}
v_0(a,b)=2, \quad v_1(a,b)=b, \\
v_{n+1}(a,b) = bv_n(a,b) - av_{n-1}(a,b), \quad n \geq 1.
\end{gathered} \tag{1.2}
$$

It is well known that

$$
\begin{aligned}
u_n(a,b) = \frac{1}{\sqrt{b^2-4a}}\Bigg(\Big(\frac{b+\sqrt{b^2-4a}}{2}\Big)^n \\
- \Big(\frac{b-\sqrt{b^2-4a}}{2}\Big)^n\Bigg) \quad (b^2-4a \neq 0)
\end{aligned} \tag{1.3}
$$

and

$$
v_n(a,b) = \left(\frac{b+\sqrt{b^2-4a}}{2}\right)^n + \left(\frac{b-\sqrt{b^2-4a}}{2}\right)^n. \tag{1.4}
$$

2000 AMS *Mathematics Subject Classification.* 11B39, 11B50, 11A15, 11E25.
Key words and phrases. Prime, Lucas sequence, reciprocity law.
Received by the editors on November 9, 2000, and in revised form on May 30, 2001.

Suppose that p is an odd prime. For two integers a and b, it is known that (see [**2**], [**5**])

$$u_{p-(\frac{b^2-4a}{p})}(a,b) \equiv 0 \pmod p$$

and

$$u_p(a,b) \equiv \Big(\frac{b^2-4a}{p}\Big) \pmod p,$$

where $(\frac{\cdot}{p})$ is the Legendre symbol.

Let $\{F_n\}$ be the Fibonacci sequence defined by $F_n = u_n(-1,1)$, and $p \ne 5$. In [**14**] we determined $F_{\frac{p\pm1}{2}} \pmod p$ by proving that

$$(1.5)\quad F_{\frac{p-(\frac{5}{p})}{2}} \equiv \begin{cases} 0 \pmod p & \text{if } p \equiv 1 \pmod 4, \\ 2(-1)^{[\frac{p+5}{10}]}\Big(\frac{5}{p}\Big)5^{\frac{p-3}{4}} \pmod p & \text{if } p \equiv 3 \pmod 4 \end{cases}$$

and

$$(1.6)\quad F_{\frac{p+(\frac{5}{p})}{2}} \equiv \begin{cases} (-1)^{[\frac{p+5}{10}]}\Big(\frac{5}{p}\Big)5^{\frac{p-1}{4}} \pmod p & \text{if } p \equiv 1 \pmod 4 \\ (-1)^{[\frac{p+5}{10}]}5^{\frac{p-3}{4}} \pmod p & \text{if } p \equiv 3 \pmod 4, \end{cases}$$

where $[\cdot]$ is the greatest integer function.

In [**7**] the author determined the values of $P_{\frac{p\pm1}{2}} \pmod p$ (the sequence $\{P_n\}$ is the Pell sequence defined $P_n = u_n(-1,2)$) by proving that

$$(1.7)\qquad P_{\frac{p-(\frac{2}{p})}{2}} \equiv \begin{cases} 0 \pmod p & \text{if } p \equiv 1 \pmod 4, \\ (-1)^{[\frac{p+5}{8}]}2^{\frac{p-3}{4}} \pmod p & \text{if } p \equiv 3 \pmod 4 \end{cases}$$

and

$$(1.8)\qquad P_{\frac{p+(\frac{2}{p})}{2}} \equiv (-1)^{[\frac{p+1}{8}]}2^{[\frac{p}{4}]} \pmod p.$$

Suppose $p \nmid a(b^2-4a)$, $(\frac{a}{p}) = 1$ and $m^2 \equiv a \pmod p$. In [**8**] the author showed that

$$(1.9)\qquad u_{\frac{p+1}{2}}(a,b) \equiv \begin{cases} \Big(\frac{b-2m}{p}\Big) \pmod p & \text{if } \Big(\frac{b^2-4a}{p}\Big) = 1, \\ 0 \pmod p & \text{if } \Big(\frac{b^2-4a}{p}\Big) = -1, \end{cases}$$

and

$$(1.10)\quad u_{\frac{p-1}{2}}(a,b)\equiv\begin{cases}0\pmod p & \text{if } \left(\frac{b^2-4a}{p}\right)=1,\\ \frac{1}{m}\left(\frac{b-2m}{p}\right)\pmod p & \text{if } \left(\frac{b^2-4a}{p}\right)=-1.\end{cases}$$

In this paper we will determine $u_{\frac{p\pm1}{2}}(a,b) \pmod p$ and $v_{\frac{p\pm1}{2}}(a,b) \pmod p$ on the condition that $(\frac{4a-b^2}{p})=1$ or $(\frac{-a}{p})=1$. In the case $a=-c^2$, the following reciprocity law is established.

(1.11) Let p be an odd prime such that $p\nmid c(b^2+4c^2)$ and $u_n=u_n(-c^2,b)$. Then there is a unique element $\delta_p\in\{1,-1\}$ such that

$$u_{\frac{p-(\frac{b^2+4c^2}{p})}{2}}\equiv\begin{cases}0\pmod p & \text{if } p\equiv 1\pmod 4,\\ 2c_p\,\delta_p(b^2+4c^2)^{\frac{p-3}{4}}\pmod p & \text{if } p\equiv 3\pmod 4\end{cases}$$

and

$$u_{\frac{p+(\frac{b^2+4c^2}{p})}{2}}\equiv\begin{cases}\frac{\delta_p}{c_p}(b^2+4c^2)^{\frac{p-1}{4}}\pmod p & \text{if } p\equiv 1\pmod 4,\\ \frac{\delta_p\,b}{c_p}\left(\frac{b^2+4c^2}{p}\right)(b^2+4c^2)^{\frac{p-3}{4}}\pmod p & \text{if } p\equiv 3\pmod 4,\end{cases}$$

where

$$c_p=\begin{cases}1 & \text{if } \left(\frac{b^2+4c^2}{p}\right)=1,\\ c & \text{if } \left(\frac{b^2+4c^2}{p}\right)=-1.\end{cases}$$

Furthermore, if q is also an odd prime satisfying $q\nmid c$ and $p\equiv\pm q\,(\mathrm{mod}\,(3-(-1)^b)(b^2+4c^2))$, then $\delta_p=\delta_q$.

As an application we obtain the criteria for $p\mid u_{\frac{p-1}{4}}(a,b)$ (if $p\equiv 1 \pmod 4$ is a prime). In particular we have the following result.

(1.12) Let $p\equiv 1\pmod 4$ be a prime, and b be odd with $b^2+4\neq p$. If $p=x^2+(b^2+4)y^2$ for some integers x and y, then $p\mid u_{\frac{p-1}{4}}(-1,b)$ if and only if $4\mid xy$.

Let $Q_0(p)$ and $Q_1(p)$ be defined as in [**10**]. In Section 5 we also obtain the criteria for $k \in Q_0(p)$ and $k \in Q_1(p)$.

2. The case $(\frac{4a-b^2}{p}) = 1$. Let $\mathbf{Z}$ be the set of integers, $i = \sqrt{-1}$ and $\mathbf{Z}[i] = \{a + bi \mid a, b \in \mathbf{Z}\}$. For $\pi = a + bi \in \mathbf{Z}[i]$ the norm of π is given by $N\pi = \pi\bar{\pi} = a^2 + b^2$. Here $\bar{\pi}$ means the complex conjugate of π. When $b \equiv 0 \pmod 2$ and $a + b \equiv 1 \pmod 4$ we say that π is primary.

If π or $-\pi$ is primary in $\mathbf{Z}[i]$, then we may write $\pi = \pm\pi_1\pi_2\cdots\pi_r$, where $\pi_1, \dots, \pi_r$ are primary primes. For $a \in \mathbf{Z}[i]$ the quartic Jacobi symbol $(\frac{\alpha}{\pi})_4$ is defined by $(\frac{\alpha}{\pi})_4 = (\frac{\alpha}{\pi_1})_4 \cdots (\frac{\alpha}{\pi_r})_4$, where $(\frac{\alpha}{\pi_s})_4$ is the quartic residue character of α modulo π_s which is given by

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

According to [**3**, pp. 123, 311] or [**1**, pp. 242–243, 247] the quartic Jacobi symbol has the following properties:

(2.1) If $a + bi$ is primary in $\mathbf{Z}[i]$, then

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

(2.2) If α and π are relatively prime primary elements in $\mathbf{Z}[i]$, then

$$\overline{\left(\frac{\alpha}{\pi}\right)_4} = \left(\frac{\alpha}{\pi}\right)_4^{-1} = \left(\frac{\bar{\alpha}}{\bar{\pi}}\right)_4.$$

(2.3) If $a + bi$ and $c + di$ are relatively prime primary elements in $\mathbf{Z}[i]$, then

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

Now we can give

Theorem 2.1. *Let p be an odd prime, $a, b \in \mathbf{Z}$, $p \nmid a$, $(\frac{4a-b^2}{p}) = 1$ and $s^2 \equiv 4a - b^2 \pmod p$ $(s \in \mathbf{Z})$. Then*

$$u_{\frac{p-(\frac{-1}{p})}{2}}(a,b) \equiv \begin{cases} 0 \pmod p & \text{if } \left(\frac{a}{p}\right) = 1, \\ \frac{2}{s}\left(\frac{-1}{p}\right)(-a)^{\frac{p-(\frac{-1}{p})}{4}}\left(\frac{s+bi}{p}\right)_4 i \pmod p & \text{if } \left(\frac{a}{p}\right) = -1, \end{cases}$$

and

$$u_{\frac{p+(\frac{-1}{p})}{2}}(a,b) \equiv \begin{cases} (-a)^{[\frac{p}{4}]}\Big(\dfrac{s+bi}{p}\Big)_4 \pmod p & \text{if } \Big(\dfrac{a}{p}\Big)=1, \\ \dfrac{b}{s}\,(-a)^{[\frac{p}{4}]}\Big(\dfrac{s+bi}{p}\Big)_4\, i \pmod p & \text{if } \Big(\frac{a}{p}\Big)=-1. \end{cases}$$

Proof. From [**10**, Lemma 2.1] we see that

$$\Big(\frac{s+bi}{p}\Big)_4^2 = \Big(\frac{s^2+b^2}{p}\Big) = \Big(\frac{4a}{p}\Big) = \Big(\frac{a}{p}\Big).$$

Thus, if $(\frac{a}{p})=-1$, then

$$\Big(\frac{s+bi}{p}\Big)_4 = \Big(\frac{s+bi}{p}\Big)_4^{-1} = \pm 1;$$

if $(\frac{a}{p})=-1$, then

$$\Big(\frac{s+bi}{p}\Big)_4 = -\Big(\frac{s+bi}{p}\Big)_4^{-1} = \pm\, i.$$

If $p\equiv 1 \pmod 4$, then $t^2\equiv -1 \pmod p$ for some integer t. Hence by (1.3) we have

$$\begin{aligned} u_n(a,b) &= \frac{1}{\sqrt{b^2-4a}}\bigg(\Big(\frac{b+\sqrt{b^2-4a}}{2}\Big)^n - \Big(\frac{b-\sqrt{b^2-4a}}{2}\Big)^n\bigg) \\ &= \frac{2}{2^n\sqrt{b^2-4a}}\sum_{r=0}^{[(n-1)/2]}\binom{n}{2r+1} b^{n-2r-1}\big(\sqrt{b^2-4a}\big)^{2r+1} \\ &= \frac{2}{2^n}\sum_{r=0}^{[(n-1)/2]}\binom{n}{2r+1} b^{n-2r-1}(b^2-4a)^r \\ &\equiv \frac{2}{2^n}\sum_{r=0}^{[(n-1)/2]}\binom{n}{2r+1} b^{n-2r-1}\Big(\frac{s}{t}\Big)^{2r+1}\frac{t}{s} \\ &= \frac{t}{s}\left\{\Big(\frac{b+s/t}{2}\Big)^n - \Big(\frac{b-s/t}{2}\Big)^n\right\} \\ &= \frac{t}{(2t)^n s}\big\{(s+bt)^n + (-1)^{n-1}(s-bt)^n\big\} \pmod p. \end{aligned}$$

Suppose $p = x^2 + y^2$ $(x, y \in \mathbf{Z})$ with $2 \mid y$ and $x + y \equiv 1 \pmod 4$. Clearly we may choose the sign of y so that $y \equiv xt \pmod p$. For $\pi = x + yi$ it is easily seen that $N\pi = p$ and $t \equiv y/x \equiv i \pmod \pi$. So by using (2.2), we get

$$\begin{aligned}\Big(\frac{s+bi}{p}\Big)_4 &= \Big(\frac{s+bi}{\pi}\Big)_4\Big(\frac{s+bi}{\bar\pi}\Big)_4 \\ &= \Big(\frac{s+bi}{\pi}\Big)_4\overline{\Big(\frac{s-bi}{\pi}\Big)_4} = \Big(\frac{s+bi}{\pi}\Big)_4\Big(\frac{s-bi}{\pi}\Big)_4^{-1} \\ &\equiv \Big(\frac{s+bi}{s-bi}\Big)^{\frac{p-1}{4}} \equiv \Big(\frac{s+bt}{s-bt}\Big)^{\frac{p-1}{4}} \pmod \pi.\end{aligned}$$

It then follows that

$$(s+bt)^{\frac{p-1}{2}} \equiv (s^2-b^2t^2)^{\frac{p-1}{4}}\Big(\frac{s+bi}{p}\Big)_4 \equiv (4a)^{\frac{p-1}{4}}\Big(\frac{s+bi}{p}\Big)_4 \pmod \pi$$

and so that

$$(s-bt)^{\frac{p-1}{2}} = \Big(\frac{s^2-b^2t^2}{s+bt}\Big)^{\frac{p-1}{2}} \equiv (4a)^{\frac{p-1}{4}}\Big(\frac{s+bi}{p}\Big)_4^{-1} \pmod \pi.$$

Recall that $t \equiv i \pmod \pi$. By the above we obtain

$$\begin{aligned}u_{\frac{p-1}{2}}(a,b) &\equiv \frac{t}{(2t)^{\frac{p-1}{2}}s}\Big\{(s+bt)^{\frac{p-1}{2}} - (s-bt)^{\frac{p-1}{2}}\Big\} \\ &\equiv \frac{t}{s}(-a)^{\frac{p-1}{4}}\Big\{\Big(\frac{s+bi}{p}\Big)_4 - \Big(\frac{s+bi}{p}\Big)_4^{-1}\Big\} \\ &\equiv \begin{cases} 0 \pmod p & \text{if } \big(\frac{a}{p}\big) = 1, \\ \frac{i}{s}(-a)^{\frac{p-1}{4}}\cdot 2\Big(\frac{s+bi}{p}\Big)_4 \pmod \pi & \text{if } \big(\frac{a}{p}\big) = -1\end{cases}\end{aligned}$$

and

$$\begin{aligned} u_{\frac{p+1}{2}}(a,b) &\equiv \frac{t}{(2t)^{\frac{p+1}{2}}s}\left\{(s+bt)^{\frac{p+1}{2}}+(s-bt)^{\frac{p+1}{2}}\right\} \\ &\equiv \frac{(4a)^{\frac{p-1}{4}}t}{(2t)^{\frac{p+1}{2}}s}\left\{(s+bt)\left(\frac{s+bi}{p}\right)_4+(s-bt)\left(\frac{s+bi}{p}\right)_4^{-1}\right\} \\ &\equiv \frac{1}{2s}(-a)^{\frac{p-1}{4}}\left\{(s+bt)\left(\frac{s+bi}{p}\right)_4+(s-bt)\left(\frac{s+bi}{p}\right)_4^{-1}\right\} \\ &\equiv \begin{cases} (-a)^{\frac{p-1}{4}}\left(\frac{s+bi}{p}\right)_4 \pmod{\pi} & \text{if } \left(\frac{a}{p}\right)=1, \\ \frac{b}{s}(-a)^{\frac{p-1}{4}}\left(\frac{s+bi}{p}\right)_4 i \pmod{\pi} & \text{if } \left(\frac{a}{p}\right)=-1. \end{cases} \end{aligned}$$

Since both sides of the above congruences are rational, the congruences are also true when π is replaced by $p\,(=N\pi)$.

If $p \equiv 3 \pmod 4$, one can similarly prove that

$$u_n(a,b) \equiv \frac{i}{(2i)^n s}\left\{(s+bi)^n+(-1)^{n-1}(s-bi)^n\right\} \pmod{p}.$$

Since $(s+bi)^p \equiv s-bi \pmod{p}$, we see that

$$\left(\frac{s+bi}{p}\right)_4 \equiv (s+bi)^{\frac{p(p+1)}{4}-\frac{p+1}{4}} \equiv \left(\frac{s-bi}{s+bi}\right)^{\frac{p+1}{4}} \pmod{p}.$$

Thus,

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

and

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

Hence,

$$\begin{aligned} u_{\frac{p+1}{2}}(a,b) &\equiv \frac{i}{(2i)^{\frac{p+1}{2}}s}(4a)^{\frac{p+1}{4}}\left\{\left(\frac{s+bi}{p}\right)_4^{-1}-\left(\frac{s+bi}{p}\right)_4\right\} \\ &= \begin{cases} 0 \pmod{p} & \text{if } \left(\frac{a}{p}\right)=1, \\ -\frac{2}{s}(-a)^{\frac{p+1}{4}}\left(\frac{s+bi}{p}\right)_4 i \pmod{p} & \text{if } \left(\frac{a}{p}\right)=-1 \end{cases} \end{aligned}$$

and

$$\begin{aligned}u_{\frac{p-1}{2}}(a,b) &\equiv \frac{i}{(2i)^{\frac{p-1}{2}}s}\Big\{(s+bi)^{\frac{p-1}{2}}+(s-bi)^{\frac{p-1}{2}}\Big\}\\ &\equiv \frac{i}{(2i)^{\frac{p-1}{2}}s}(4a)^{\frac{p+1}{4}}\Big\{\Big(\frac{s+bi}{p}\Big)_4^{-1}\frac{1}{s+bi}+\Big(\frac{s+bi}{p}\Big)_4\frac{1}{s-bi}\Big\}\\ &\equiv \begin{cases}(-a)^{\frac{p-3}{4}}\Big(\frac{s+bi}{p}\Big)_4 \pmod p & \text{if } \Big(\frac{a}{p}\Big)=1,\\ \frac{b}{s}(-a)^{\frac{p-3}{4}}\Big(\frac{s+bi}{p}\Big)_4 i \pmod p & \text{if } \Big(\frac{a}{p}\Big)=-1.\end{cases}\end{aligned}$$

Combining the above we obtain the result.

Corollary 2.1. *Let p be an odd prime, $a, b \in \mathbf{Z}$, $p \nmid a$, $(\frac{4a-b^2}{p}) = 1$ and $s^2 \equiv 4a - b^2 \pmod p$ for $s \in \mathbf{Z}$. Then*

$$v_{\frac{p-(\frac{-1}{p})}{2}}(a,b) \equiv \begin{cases}2(-a)^{\frac{p-(\frac{-1}{p})}{4}}\Big(\frac{s+bi}{p}\Big)_4 \pmod p & \text{if } \Big(\frac{a}{p}\Big)=1,\\ 0 \pmod p & \text{if } \Big(\frac{a}{p}\Big)=-1,\end{cases}$$

and

$$v_{\frac{p+(\frac{-1}{p})}{2}}(a,b) \equiv \begin{cases}\Big(\frac{-1}{p}\Big)(-a)^{[\frac{p}{4}]}b\Big(\frac{s+bi}{p}\Big)_4 \pmod p & \text{if } \Big(\frac{a}{p}\Big)=1,\\ -\Big(\frac{-1}{p}\Big)(-a)^{[\frac{p}{4}]}s\Big(\frac{s+bi}{p}\Big)_4 i \pmod p & \text{if } \Big(\frac{a}{p}\Big)=-1.\end{cases}$$

Proof. Let $u_n = u_n(a,b)$ and $v_n = v_n(a,b)$. It follows from (1.3) and (1.4) that $u_n = (2v_{n+1} - bv_n)/(b^2 - 4a)$ and $v_n = 2u_{n+1} - bu_n = bu_n - 2au_{n-1}$ $(n \ge 1)$. Thus,

(2.4) $$v_{\frac{p-1}{2}} = 2u_{\frac{p+1}{2}} - bu_{\frac{p-1}{2}} \quad \text{and} \quad v_{\frac{p+1}{2}} = bu_{\frac{p+1}{2}} - 2au_{\frac{p-1}{2}}.$$

This together with Theorem 2.1 proves the corollary.

3. The case $(\frac{-a}{p}) = 1$.

Lemma 3.1. *Let p be an odd prime, $a, b \in \mathbf{Z}$ and $a' = \frac{b^2-4a}{4}$. Then*

(i) $$u_{\frac{p-1}{2}}(a,b) \equiv -\left(\frac{2}{p}\right) u_{\frac{p-1}{2}}(a',b) \pmod p;$$

(ii) $$u_{\frac{p+1}{2}}(a,b) \equiv \frac{1}{2}\left(\frac{2}{p}\right) v_{\frac{p-1}{2}}(a',b) \pmod p;$$

(iii) $$v_{\frac{p-1}{2}}(a,b) \equiv 2\left(\frac{2}{p}\right) u_{\frac{p+1}{2}}(a',b) \pmod p;$$

(iv) $$v_{\frac{p+1}{2}}(a,b) \equiv \left(\frac{2}{p}\right) v_{\frac{p+1}{2}}(a',b) \pmod p.$$

Proof. By induction one can easily prove the following known result, see [**6**]:

$$u_{n+1}(a,b) = \sum_{r=0}^{[n/2]} \binom{n-r}{r} (-a)^r\, b^{n-2r}, \quad n \geq 0.$$

For $r = 0, 1, \ldots, [\frac{p-1}{4}]$ it is clear that

$$\binom{\frac{p-1}{2}-r}{r} \Big/ \binom{\frac{p-1}{2}}{2r} = \frac{(2r)!}{\frac{p-1}{2}\cdot\frac{p-3}{2}\cdots(\frac{p-1}{2}-r+1)\cdot r!} \equiv \frac{(-2)^r\cdot(2r)!}{1\cdot 3\cdots(2r-1)\cdot r!} = (-4)^r \pmod p.$$

Thus,

$$\begin{aligned} u_{\frac{p+1}{2}}(a,b) &= \sum_{r=0}^{[(p-1)/4]} \binom{\frac{p-1}{2}-r}{r} (-a)^r\, b^{\frac{p-1}{2}-2r} \\ &\equiv \sum_{r=0}^{[(p-1)/4]} \binom{\frac{p-1}{2}}{2r} (b^2-4a')^r\, b^{\frac{p-1}{2}-2r} \\ &= \frac{1}{2}\left\{\left(b+\sqrt{b^2-4a'}\right)^{\frac{p-1}{2}} + \left(b-\sqrt{b^2-4a'}\right)^{\frac{p-1}{2}}\right\} \\ &= 2^{\frac{p-1}{2}-1} v_{\frac{p-1}{2}}(a',b) \equiv \frac{1}{2}\left(\frac{2}{p}\right) v_{\frac{p-1}{2}}(a',b) \pmod p \end{aligned}$$

and hence

$$u_{\frac{p+1}{2}}(a',b) \equiv \frac{1}{2}\Big(\frac{2}{p}\Big)v_{\frac{p-1}{2}}\Big(\frac{b^2-4a'}{4},b\Big) \pmod p.$$

That is,

$$v_{\frac{p-1}{2}}(a,b) \equiv 2\Big(\frac{2}{p}\Big)u_{\frac{p+1}{2}}(a',b) \pmod p.$$

If $p \nmid b$, by using (2.4) and the above we derive

$$\begin{aligned} u_{\frac{p-1}{2}}(a,b) &= \frac{1}{b}(2u_{\frac{p+1}{2}}(a,b) - v_{\frac{p-1}{2}}(a,b)) \\ &\equiv \frac{1}{b}\Big(\frac{2}{p}\Big)v_{\frac{p-1}{2}}(a',b) - \frac{2}{b}\Big(\frac{2}{p}\Big)u_{\frac{p+1}{2}}(a',b) \\ &= -\Big(\frac{2}{p}\Big)u_{\frac{p-1}{2}}(a',b) \pmod p. \end{aligned}$$

If $p \mid b$, by using (1.3) we also have

$$\begin{aligned} u_{\frac{p-1}{2}}(a,b) &\equiv \frac{1}{2\sqrt{-a}}\Big\{(\sqrt{-a}\,)^{\frac{p-1}{2}} - (-\sqrt{-a}\,)^{\frac{p-1}{2}}\Big\} \\ &= -\Big(\frac{2}{p}\Big)\cdot\frac{1}{2\sqrt{a}}\Big\{(\sqrt{a}\,)^{\frac{p-1}{2}} - (-\sqrt{a}\,)^{\frac{p-1}{2}}\Big\} \\ &\equiv -\Big(\frac{2}{p}\Big)u_{\frac{p-1}{2}}(a',b) \pmod p. \end{aligned}$$

Hence

$$\begin{aligned} v_{\frac{p+1}{2}}(a,b) &= bu_{\frac{p+1}{2}}(a,b) - 2au_{\frac{p-1}{2}}(a,b) \\ &\equiv \frac{b}{2}\Big(\frac{2}{p}\Big)v_{\frac{p-1}{2}}(a',b) + 2a\Big(\frac{2}{p}\Big)u_{\frac{p-1}{2}}(a',b) \\ &= \Big(\frac{2}{p}\Big)v_{\frac{p+1}{2}}(a',b) \pmod p. \end{aligned}$$

The proof is now complete.

We are now ready to give

Theorem 3.1. *Let p be an odd prime, $a,b \in \mathbf{Z}$, $p \nmid a(b^2-4a)$, $(\frac{-a}{p}) = 1$ and $c^2 \equiv -a \pmod p$ for $c \in \mathbf{Z}$.*

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

$$u_{\frac{p-1}{2}}(a,b)\equiv\begin{cases}0 \pmod p & \textit{if } \left(\frac{b^2-4a}{p}\right)=1,\\ -\frac{1}{c}\,(b^2-4a)^{\frac{p-1}{4}}\left(\frac{b-2ci}{p}\right)_4 i \pmod p & \textit{if } \left(\frac{b^2-4a}{p}\right)=-1,\end{cases}$$

and

$$u_{\frac{p+1}{2}}(a,b)\equiv\begin{cases}(b^2-4a)^{\frac{p-1}{4}}\left(\frac{b-2ci}{p}\right)_4 \pmod p & \textit{if } \left(\frac{b^2-4a}{p}\right)=1,\\ 0 \pmod p & \textit{if } \left(\frac{b^2-4a}{p}\right)=-1.\end{cases}$$

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

$$u_{\frac{p-1}{2}}(a,b)\equiv\begin{cases}2(b^2-4a)^{\frac{p-3}{4}}\left(\frac{b-2ci}{p}\right)_4 \pmod p & \textit{if } \left(\frac{b^2-4a}{p}\right)=1,\\ \frac{b}{c}\,(b^2-4a)^{\frac{p-3}{4}}\left(\frac{b-2ci}{p}\right)_4 i \pmod p & \textit{if } \left(\frac{b^2-4a}{p}\right)=-1\end{cases}$$

and

$$u_{\frac{p+1}{2}}(a,b)\equiv\begin{cases}b(b^2-4a)^{\frac{p-3}{4}}\left(\frac{b-2ci}{p}\right)_4 \pmod p & \textit{if } \left(\frac{b^2-4a}{p}\right)=1,\\ -2c(b^2-4a)^{\frac{p-3}{4}}\left(\frac{b-2ci}{p}\right)_4 i \pmod p & \textit{if } \left(\frac{b^2-4a}{p}\right)=-1.\end{cases}$$

Proof. Let $a'\in\mathbf{Z}$ be such that $a'\equiv\frac{b^2-4a}{4} \pmod p$. Then clearly $(2c)^2\equiv -4a\equiv 4a'-b^2 \pmod p$. Also, $u_n(a',b)\equiv u_n((b^2-4a)/4,b) \pmod p$ and $v_n(a',b)\equiv v_n((b^2-4a)/4,b) \pmod p$. Now, using Theorem 2.1 and Corollary 2.1 for the Lucas sequence $\{u_n(a',b)\}$ and then applying Lemma 3.1 and the fact that

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

we obtain the result.

Remark 3.1. Suppose that p is a prime of the form $4n+3$, $b, c \in \mathbf{Z}$, $p \nmid c$ and $(\frac{b^2+4c^2}{p}) = -1$. In [**11**] the author proved that

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

Now it is an easy consequence of Theorem 3.1.

Corollary 3.1. *Let p be an odd prime, $a, b \in \mathbf{Z}$, $p \nmid a(b^2-4a)$, $(\frac{-a}{p}) = 1$ and $c^2 \equiv -a \pmod p$ for $c \in \mathbf{Z}$.*

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

$$v_{\frac{p-1}{2}}(a,b) \equiv \begin{cases} 2(b^2-4a)^{\frac{p-1}{4}}\Big(\frac{b-2ci}{p}\Big)_4 \pmod p & \text{if } \Big(\frac{b^2-4a}{p}\Big)=1, \\ \frac{b}{c}(b^2-4a)^{\frac{p-1}{4}}\Big(\frac{b-2ci}{p}\Big)_4 i \pmod p & \text{if } \Big(\frac{b^2-4a}{p}\Big)=-1 \end{cases}$$

and

$$v_{\frac{p+1}{2}}(a,b) \equiv \begin{cases} b(b^2-4a)^{\frac{p-1}{4}}\Big(\frac{b-2ci}{p}\Big)_4 \pmod p & \textit{if } \Big(\frac{b^2-4a}{p}\Big)=1, \\ -2c(b^2-4a)^{\frac{p-1}{4}}\Big(\frac{b-2ci}{p}\Big)_4 i \pmod p & \textit{if } \Big(\frac{b^2-4a}{p}\Big)=-1. \end{cases}$$

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

$$v_{\frac{p-1}{2}}(a,b) \equiv \begin{cases} 0 \pmod p & \textit{if } \Big(\frac{b^2-4a}{p}\Big)=1, \\ -\frac{1}{c}(b^2-4a)^{\frac{p+1}{4}}\Big(\frac{b-2ci}{p}\Big)_4 i \pmod p & \textit{if } \Big(\frac{b^2-4a}{p}\Big)=-1, \end{cases}$$

and

$$v_{\frac{p+1}{2}}(a,b) \equiv \begin{cases} (b^2-4a)^{\frac{p+1}{4}}\Big(\frac{b-2ci}{p}\Big)_4 \pmod p & \textit{if } \Big(\frac{b^2-4a}{p}\Big)=1, \\ 0 \pmod p & \textit{if } \Big(\frac{b^2-4a}{p}\Big)=-1. \end{cases}$$

Proof. This is immediate from (2.4) and Theorem 3.1.

4. The reciprocity law for $u_{\frac{p\pm1}{2}}(-c^2, b) \pmod p$.

Lemma 4.1. *Let p and q be two positive odd numbers, $b, c \in \mathbf{Z}$, $gcd\,(b^2+4c^2, pq) = 1$ and $p \equiv \pm q (\mathrm{mod}\,(3-(-1)^b)(b^2+4c^2))$. Then*

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

Proof. If $b \equiv 1 \pmod 2$, then $(-1)^{\frac{b-1}{2}+c}(b+2ci)$ is primary. Using (2.3), we see that

$$\begin{aligned}\Big(\frac{b+2ci}{p}\Big)_4 &= \Big(\frac{(-1)^{\frac{b-1}{2}+c}(b+2ci)}{(-1)^{\frac{p-1}{2}}p}\Big)_4 = \Big(\frac{(-1)^{\frac{p-1}{2}}p}{(-1)^{\frac{b-1}{2}+c}(b+2ci)}\Big)_4 \\ &= \Big(\frac{(-1)^{\frac{q-1}{2}}q}{(-1)^{\frac{b-1}{2}+c}(b+2ci)}\Big)_4 = \Big(\frac{b+2ci}{q}\Big)_4.\end{aligned}$$

If $b \equiv 0 \pmod 2$, then clearly

$$(3-(-1)^b)(b^2+4c^2) = 2(b^2+4c^2) = 8((b/2)^2+c^2).$$

Thus, according to the proof of Theorem 2.1 of [**10**] we have

$$\Big(\frac{b+2ci}{p}\Big)_4 = \Big(\frac{b/2+ci}{p}\Big)_4 = \Big(\frac{b/2+ci}{q}\Big)_4 = \Big(\frac{b+2ci}{q}\Big)_4.$$

This completes the proof.

Now we present the following reciprocity law for $u_{\frac{p\pm1}{2}}(-c^2, b) \pmod p$.

Theorem 4.1. *Let $b, c \in \mathbf{Z}$, $u_0 = 0$, $u_1 = 1$, $u_{n+1} = bu_n + c^2u_{n-1}$ $(n \geq 1)$, and let p be an odd prime such that $p \nmid c(b^2+4c^2)$. Then there is a unique element $\delta_p \in \{1, -1\}$ such that*

$$u_{\frac{p-(\frac{b^2+4c^2}{p})}{2}} \equiv \begin{cases} 0 \pmod p & \text{if } p \equiv 1 \pmod 4, \\ 2c_p\,\delta_p(b^2+4c^2)^{\frac{p-3}{4}} \pmod p & \text{if } p \equiv 3 \pmod 4)\end{cases}$$

and

$$u_{\frac{p+(\frac{b^2+4c^2}{p})}{2}} \equiv \begin{cases} \frac{\delta_p}{c_p}(b^2+4c^2)^{\frac{p-1}{4}} \pmod p & \text{if } p\equiv 1 \pmod 4,\\ \frac{b\,\delta_p}{c_p}\Big(\frac{b^2+4c^2}{p}\Big)(b^2+4c^2)^{\frac{p-3}{4}} \pmod p & \text{if } p\equiv 3 \pmod 4,\end{cases}$$

where

$$c_p = \begin{cases} 1 & \text{if} \Big(\frac{b^2+4c^2}{p}\Big)=1,\\ c & \text{if} \Big(\frac{b^2+4c^2}{p}\Big)=-1.\end{cases}$$

Furthermore, if q is also an odd prime satisfying $q \nmid c$ and $p \equiv \pm q (\bmod\,(3-(-1)^b)(b^2+4c^2))$, then $\delta_p=\delta_q$. Moreover,

$$\delta_p = \begin{cases} \Big(\frac{b+2ci}{p}\Big)_4 & \text{if} \Big(\frac{b^2+4c^2}{p}\Big)=1,\\ \Big(\frac{b+2ci}{p}\Big)_4 i & \text{if} \Big(\frac{b^2+4c^2}{p}\Big)=-1.\end{cases} \tag{4.1}$$

Proof. Let δ_p be defined by (4.1). Since $(\frac{b+2ci}{p})_4^2=(\frac{b^2+4c^2}{p})$ by [**10**, Lemma 2.1] we see that $\delta_p\in\{1,-1\}$ and

$$\begin{aligned}\Big(\frac{b-2ci}{p}\Big)_4 &= \overline{\Big(\frac{b+2ci}{p}\Big)_4} = \Big(\frac{b+2ci}{p}\Big)_4^{-1} = \Big(\frac{b+2ci}{p}\Big)_4^3\\ &= \Big(\frac{b+2ci}{p}\Big)_4\Big(\frac{b^2+4c^2}{p}\Big).\end{aligned}$$

So

$$\delta_p = \begin{cases} \Big(\frac{b-2ci}{p}\Big)_4 & \text{if } \Big(\frac{b^2+4c^2}{p}\Big)=1,\\ -\big(\frac{b-2ci}{p}\big)_4 i & \text{if } \Big(\frac{b^2+4c^2}{p}\Big)=-1.\end{cases}$$

Now putting $a=-c^2$ in Theorem 3.1, we see that the congruences in Theorem 4.1 hold.

If q is also an odd prime satisfying $q \nmid c$ and $p \equiv \pm q (\mathrm{mod}\, (3-(-1)^b)(b^2+4c^2))$, then $(\frac{b+2ci}{p})_4 = (\frac{b+2ci}{q})_4$ by Lemma 4.1. Since

$$\Big(\frac{b+2ci}{p}\Big)_4^2 = \Big(\frac{b^2+4c^2}{p}\Big) \quad \text{and} \quad \Big(\frac{b+2ci}{q}\Big)_4^2 = \Big(\frac{b^2+4c^2}{q}\Big),$$

we see that $\delta_p = \delta_q$. Hence the theorem is proved.

Remark 4.1. (1) We note that the appearance of all the zero-values modulo p in Theorems 2.1, 3.1 and 4.1 can be inferred from the following result given in [**4**, p. 441], which is due to Lehmer. If $a, b \in \mathbf{Z}$, $(\frac{a}{p}) = 1$ and $p \nmid b^2 - 4a$, then

$$u_{\frac{p-(\frac{b^2-4a}{p})}{2}}(a,b) \equiv 0 \pmod p.$$

(2) In a similar way one can establish a reciprocity law for the Lucas sequence $\{u_n(\frac{b^2+c^2}{4}, b)\}$ where b and c are integers.

(3) Suppose that $p > 3$ is a prime and that a and b are integers. For the values of $u_{\frac{p-(\frac{p}{3})}{3}}(a,b) \pmod p$ one may consult [**9**] and [**13**].

Let δ_p and c_p be defined as in Theorem 4.1. From Theorem 4.1, we see that

(4.2)

$$\delta_p \equiv \begin{cases} c_p(b^2+4c^2)^{-\frac{p-1}{4}} u_{\frac{p+(\frac{b^2+4c^2}{p})}{2}}(-c^2,b) \pmod p & \text{if } p\equiv 1 \pmod 4, \\ \dfrac{c_p}{b}(b^2+4c^2)^{\frac{p+1}{4}} u_{\frac{p+(\frac{b^2+4c^2}{p})}{2}}(-c^2,b) \pmod p & \text{if } p\equiv 3 \pmod 4. \end{cases}$$

Thus, putting $b = c = 1$ we find $\delta_3 = -1$, $\delta_7 = 1$, $\delta_{11} = -1$ and $\delta_{19} = 1$. Hence

$$\begin{aligned} \delta_p &= \begin{cases} \delta_3 = -1 & \text{if } p \equiv \pm 3 \pmod{20}, \\ \delta_7 = 1 & \text{if } p \equiv \pm 7 \pmod{20}, \\ \delta_{11} = -1 & \text{if } p \equiv \pm 9 \pmod{20}, \\ \delta_{19} = 1 & \text{if } p \equiv \pm 1 \pmod{20} \end{cases} \\ &= (-1)^{[\frac{p+5}{10}]}\Big(\frac{p}{5}\Big). \end{aligned}$$

Applying Theorem 4.1 gives (1.5) and (1.6).

Taking $b = 2$ and $c = 1$ in (4.2) we find $\delta_3 = 1$, $\delta_5 = -1$, $\delta_7 = -1$ and $\delta_{17} = 1$. Hence

$$\delta_p = \begin{cases} \delta_3 = 1 & \text{if } p \equiv \pm 3 \pmod{16}, \\ \delta_5 = -1 & \text{if } p \equiv \pm 5 \pmod{16}, \\ \delta_7 = -1 & \text{if } p \equiv \pm 7 \pmod{16}, \\ \delta_{17} = 1 & \text{if } p \equiv \pm 1 \pmod{16} \end{cases}$$
$$= (-1)^{[\frac{p+3}{8}]}.$$

Using Theorem 4.1 yields (1.7) and (1.8).

Corollary 4.1. *Let $u_0 = 0$, $u_1 = 1$, $u_{n+1} = 3u_n + u_{n-1}$ $(n \geq 1)$ and let $p \neq 3, 13$ be an odd prime. Then*

$$u_{\frac{p-(\frac{13}{p})}{2}} \equiv \begin{cases} 0 \pmod p & \text{if } p \equiv 1 \pmod 4, \\ 2\delta_p \cdot 13^{\frac{p-3}{4}} \pmod p & \text{if } p \equiv 3 \pmod 4 \end{cases}$$

and

$$u_{\frac{p+(\frac{13}{p})}{2}} \equiv \begin{cases} \delta_p \cdot 13^{\frac{p-1}{4}} \pmod p & \text{if } p \equiv 1 \pmod 4, \\ 3\delta_p \left(\frac{13}{p}\right) \cdot 13^{\frac{p-3}{4}} \pmod p & \text{if } p \equiv 3 \pmod 4, \end{cases}$$

where

$$\delta_p = \begin{cases} 1 & \text{if } p \equiv \pm 1, \pm 5, \pm 7, \pm 9, \pm 11, \pm 23 \pmod{52}, \\ -1 & \text{if } p \equiv \pm 3, \pm 15, \pm 17, \pm 19, \pm 21, \pm 25 \pmod{52}. \end{cases}$$

Proof. Putting $b = 3$ and $c = 1$ in (4.2), we see that

$$\delta_{53} = \delta_5 = \delta_7 = \delta_{43} = \delta_{11} = \delta_{23} = 1$$

and

$$\delta_{101} = \delta_{37} = \delta_{17} = \delta_{19} = \delta_{31} = \delta_{79} = -1.$$

Thus, applying Theorem 4.1 we obtain the result.

5. The criteria for $k \in Q_r(p)$ and $p \mid u_{\frac{p-1}{4}}(a,b)$. For positive integer p, let S_p denote the set of those rational numbers whose denominator is prime to p. Following [**10**], define

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

Now, using Theorem 3.1 we give the following criteria for $k \in Q_0(p)$ and $k \in Q_1(p)$.

Theorem 5.1. *Let p be an odd prime and $k \in \mathbf{Z}$ with $k^2 \not\equiv 0, \pm 1 \pmod p$. Then*

(i) $k \in Q_0(p)$ *if and only if*

$$u_{\frac{p+1}{2}}(-1, 2k) \equiv \begin{cases} (-k^2-1)^{\frac{p-1}{4}} \pmod p & \text{if } p \equiv 1 \pmod 4, \\ -k(-k^2-1)^{\frac{p-3}{4}} \pmod p & \text{if } p \equiv 3 \pmod 4. \end{cases}$$

(ii) $k \in Q_1(p)$ *if and only if*

$$u_{\frac{p-1}{2}}(-1, 2k) \equiv \begin{cases} -(-k^2-1)^{\frac{p-1}{4}} \pmod p & \text{if } p \equiv 1 \pmod 4, \\ -k(-k^2-1)^{\frac{p-3}{4}} \pmod p & \text{if } p \equiv 3 \pmod 4. \end{cases}$$

Proof. Let $a = -1$, $b = 2k$ and $c = -1$. Then clearly

$$b^2 - 4a = 4(k^2+1) \quad \text{and} \quad \left(\frac{b-2ci}{p}\right)_4 = \left(\frac{2k+2i}{p}\right)_4 = \left(\frac{k+i}{p}\right)_4.$$

Note that $2^{\frac{p-1}{2}} \equiv (\frac{2}{p}) = (-1)^{[\frac{p+1}{4}]} \pmod p$ and $(\frac{k+i}{p})_4^2 = (\frac{k^2+1}{p})$ by [**10**, Lemma 2.1]. Applying the above and Theorem 3.1, we obtain the desired result.

Let $p \equiv 1 \pmod 4$ be a prime, $a, b \in \mathbf{Z}$, $p \nmid a(b^2-4a)$ and $(\frac{a}{p}) = (\frac{b^2-4a}{p}) = 1$. It follows from Remark 4.1 that $p \mid u_{\frac{p-1}{2}}(a,b)$.

Since $u_{2n}(a,b) = u_n(a,b)v_n(a,b)$ (see [**5**]), we see that $p|u_{\frac{p-1}{4}}(a,b)$ or $p \mid v_{\frac{p-1}{4}}(a,b)$.

Now we give the criteria for $p|u_{\frac{p-1}{4}}(a,b)$.

Theorem 5.2. *Let* $p \equiv 1 \pmod 4$ *be a prime,* $a, b \in \mathbf{Z}$*,* $p \nmid a(b^2-4a)$*,* $(\frac{-a}{p}) = (\frac{4a-b^2}{p}) = 1$*,* $c^2 \equiv -a \pmod p$ *and* $s^2 \equiv 4a-b^2 \pmod p$*. Then the following statements are equivalent*:

(i) $$p \mid u_{\frac{p-1}{4}}(a,b);$$

(ii) $$\Big(\frac{s}{p}\Big) = \Big(\frac{c}{p}\Big)\Big(\frac{b+2ci}{p}\Big)_4;$$

(iii) $$\Big(\frac{b+si}{p}\Big)_4 = (-1)^{\frac{p-1}{4}}\Big(\frac{s+bi}{p}\Big)_4 = 1.$$

Proof. From [**9**, Lemma 6.1], we know that $p \mid u_n(a,b)$ if and only if $v_{2n}(a,b) \equiv 2a^n \pmod p$. So we have

$$p \mid u_{\frac{p-1}{4}}(a,b) \Longleftrightarrow v_{\frac{p-1}{2}}(a,b) \equiv 2a^{\frac{p-1}{4}} \pmod p.$$

Hence, using Corollary 3.1 and the fact that

$$(4a-b^2)^{\frac{p-1}{4}} \equiv s^{\frac{p-1}{2}} \equiv \Big(\frac{s}{p}\Big) \pmod p$$

we obtain

$$\begin{aligned} p \mid u_{\frac{p-1}{4}}(a,b) &\Longleftrightarrow 2(b^2-4a)^{\frac{p-1}{4}}\Big(\frac{b-2ci}{p}\Big)_4 \equiv 2a^{\frac{p-1}{4}} \pmod p \\ &\Longleftrightarrow (4a-b^2)^{\frac{p-1}{4}}\Big(\frac{b-2ci}{p}\Big)_4 \equiv (-a)^{\frac{p-1}{4}} \equiv \Big(\frac{c}{p}\Big) \pmod p \\ &\Longleftrightarrow \Big(\frac{s}{p}\Big) = \Big(\frac{c}{p}\Big)\Big(\frac{b-2ci}{p}\Big)_4^{-1} = \Big(\frac{c}{p}\Big)\Big(\frac{b+2ci}{p}\Big)_4. \end{aligned}$$

So (i) is equivalent to (ii).

Since $(\frac{a}{p}) = (\frac{-a}{p}) = 1$, in view of Corollary 2.1 we find that

$$\begin{aligned} p \mid u_{\frac{p-1}{4}}(a,b) &\iff v_{\frac{p-1}{2}}(a,b) \equiv 2a^{\frac{p-1}{4}} \pmod p \\ &\iff 2(-a)^{\frac{p-1}{4}}\Big(\frac{s+bi}{p}\Big)_4 \equiv 2a^{\frac{p-1}{4}} \pmod p \\ &\iff \Big(\frac{s+bi}{p}\Big)_4 = (-1)^{\frac{p-1}{4}} \\ &\iff \Big(\frac{s-bi}{p}\Big)_4 = \Big(\frac{s+bi}{p}\Big)_4^{-1} = (-1)^{\frac{p-1}{4}} \\ &\iff \Big(\frac{b+si}{p}\Big)_4 = \Big(\frac{i}{p}\Big)_4\Big(\frac{s-bi}{p}\Big)_4 = \Big(\frac{i}{p}\Big)_4(-1)^{\frac{p-1}{4}} = 1. \end{aligned}$$

Thus, (i) is equivalent to (iii). Hence the proof is complete.

Using Theorem 5.2 we can prove

Theorem 5.3. *Let $p \equiv 1 \pmod 4$ be a prime, and let b be odd with $b^2+4 \ne p$. If $p = x^2+(b^2+4)y^2$ for some $x, y \in \mathbf{Z}$, then $p \mid u_{\frac{p-1}{4}}(-1,b)$ if and only if $4 \mid xy$.*

Proof. Clearly $p \nmid b^2+4$ and $(\frac{x}{y})^2 \equiv -(b^2+4) \pmod p$. Suppose $s^2 \equiv -(b^2+4) \pmod p$, $x = 2^\alpha x_0 (2 \nmid x_0)$ and $y = 2^\beta y_0 (2 \nmid y_0)$. Then $s \equiv \pm\frac{x}{y} \pmod p$ and so $(\frac{s}{p}) = (\frac{x}{p})(\frac{y}{p})$. Using the Jacobi symbol, we see that

$$\begin{aligned} \Big(\frac{b+2i}{p}\Big)_4 &= \Big(\frac{(-1)^{\frac{b+1}{2}}(b+2i)}{p}\Big)_4 = \Big(\frac{p}{(-1)^{\frac{b+1}{2}}(b+2i)}\Big)_4 \\ &= \Big(\frac{x^2+(b^2+4)y^2}{b+2i}\Big)_4 = \Big(\frac{x^2}{b+2i}\Big)_4 = \Big(\frac{2}{b+2i}\Big)_4^{2\alpha}\Big(\frac{x_0^2}{b+2i}\Big)_4 \\ &= \Big(\frac{i^3(1+i)^2}{b+2i}\Big)_4^{2\alpha}\Big(\frac{b+2i}{|x_0|}\Big)_4^2 = \Big(\frac{i}{b+2i}\Big)_4^{2\alpha}\Big(\frac{b^2+4}{|x_0|}\Big) \\ &\qquad \text{(by using [\textbf{10}, Lemma 2.1])} \\ &= (-1)^\alpha\Big(\frac{x_0}{b^2+4}\Big) \quad \text{(by (2.1))}, \end{aligned}$$

and

$$\begin{aligned}\Big(\frac{s}{p}\Big) &= \Big(\frac{x}{p}\Big)\Big(\frac{y}{p}\Big) = \Big(\frac{2^{\alpha+\beta}}{p}\Big)\Big(\frac{x_0}{p}\Big)\Big(\frac{y_0}{p}\Big) = \Big(\frac{2}{p}\Big)^{\alpha+\beta}\Big(\frac{p}{|x_0|}\Big)\Big(\frac{p}{|y_0|}\Big)\\ &= \Big(\frac{2}{p}\Big)^{\alpha+\beta}\Big(\frac{x^2+(b^2+4)y^2}{|x_0|}\Big)\Big(\frac{x^2+(b^2+4)y^2}{|y_0|}\Big)\\ &= \Big(\frac{2}{p}\Big)^{\alpha+\beta}\Big(\frac{b^2+4}{|x_0|}\Big) = (-1)^{\frac{p-1}{4}(\alpha+\beta)}\Big(\frac{x_0}{b^2+4}\Big).\end{aligned}$$

Hence by Theorem 5.2 we have

$$p \mid u_{\frac{p-1}{4}}(-1,b) \Longleftrightarrow \Big(\frac{s}{p}\Big) = \Big(\frac{b+2i}{p}\Big)_4 \Longleftrightarrow (-1)^{\frac{p-1}{4}(\alpha+\beta)} = (-1)^{\alpha}.$$

If $\alpha = 0$, then $2 \nmid x$ and so $2 \mid y$. Clearly,

$$p = x^2 + (b^2+4)y^2 \equiv 1 + 5y^2 \equiv 3 - 2(-1)^{y/2} \pmod 8.$$

So we have $(-1)^{\frac{p-1}{4}\beta} = 1$ if and only if $4 \mid y$.

If $\beta = 0$, then $2 \nmid y$ and so $2 \mid x$. Since

$$p = x^2 + (b^2+4)y^2 \equiv x^2 + 5y^2 \equiv x^2 + 5 \equiv 3 + 2(-1)^{x/2} \pmod 8$$

we see that $(-1)^{\frac{p-1}{4}\alpha} = (-1)^{\alpha}$ if and only if $4 \mid x$.

Observe that $x \not\equiv y \pmod 2$ and hence $\alpha = 0$ or $\beta = 0$. By the above we get

$$\begin{aligned}p \mid u_{\frac{p-1}{4}}(-1,b) &\Longleftrightarrow (-1)^{\frac{p-1}{4}(\alpha+\beta)} = (-1)^{\alpha}\\ &\Longleftrightarrow 4 \mid x \quad \text{or} \quad 4 \mid y \Longleftrightarrow 4 \mid xy.\end{aligned}$$

This proves the theorem.

Remark 5.1. Let $\{F_n\}$ be the Fibonacci sequence, and let $p \equiv 1, 9 \pmod{20}$ be a prime. Then clearly $p = x^2 + 5y^2$ for some $x, y \in \mathbf{Z}$. Hence it follows from Theorem 5.3 that $p \mid F_{\frac{p-1}{4}}$ if and only if $4 \mid xy$. This result was given in [**14**].

Corollary 5.1. *Let* $p \equiv 1 \pmod 4$ *be a prime, and* b *be odd with* $b^2+4 \neq p$. *If* p *is represented by* $x^2+16(b^2+4)y^2$ *or* $16x^2+(b^2+4)y^2$, *then* $p \mid u_{\frac{p-1}{4}}(-1,b)$.

Corollary 5.2. *Let* $p \neq 13$ *be a prime of the form* $4n+1$. *Then* $p \mid u_{\frac{p-1}{4}}(-1,3)$ *if and only if* p *can be represented by* x^2+208y^2 *or* $16x^2+13y^2$.

Proof. Set $u_n = u_n(-1,3)$. If $p \mid u_{\frac{p-1}{4}}$, then $p \mid u_{\frac{p-1}{2}}$ since $u_{\frac{p-1}{2}} = u_{\frac{p-1}{4}} v_{\frac{p-1}{4}}(-1,3)$ (see [**5**]). Thus, applying Theorem 3.1, we see that $(\frac{13}{p}) = 1$. If $p = x^2+208y^2$ or $16x^2+13y^2$ $(x, y \in \mathbf{Z})$, then again $(\frac{13}{p}) = (\frac{-13}{p}) = 1$.

Now assume $(\frac{13}{p}) = 1$. Since $p \equiv 1 \pmod 4$, from the theory of binary quadratic forms we know that $p = x^2+13y^2$ for some $x, y \in \mathbf{Z}$. Hence, applying Theorem 5.3, we get

$$\begin{aligned} p \mid u_{\frac{p-1}{4}} &\iff p = x^2+13y^2 \quad \text{with} \quad 4 \mid xy \\ &\iff p = x^2+16\cdot 13y^2 \quad \text{or} \quad 16x^2+13y^2. \end{aligned}$$

This is the result.

Remark 5.2. Let $p \equiv 1 \pmod 4$ be a prime and $b \in \mathbf{Z}$ with $(\frac{b^2+4}{p}) = 1$. Then $p \mid u_{\frac{p-1}{4}}(-1,b)$ if and only if p can be represented by one of the primitive (integral) binary quadratic forms $Ax^2+2Bxy+Cy^2$ of discriminant $-4(3-(-1)^b)^2(b^2+4)$ with the condition that $2 \nmid A$ and $(\frac{(3-(-1)^b)b+Bi}{A})_4 = 1$. This result will be published in [**12**].

In the end we pose the following two conjectures. The two conjectures have been checked for all primes less than 3000.

Conjecture 5.1 (see [**8**]). *Let* $p \equiv 3 \pmod 8$ *be a prime, and hence* $p = x^2+2y^2$ *for some integers* x *and* y. *If* P_n *is the Pell sequence given by* $P_0 = 0$, $P_1 = 1$ *and* $P_{n+1} = 2P_n + P_{n-1}$ $(n \geq 1)$, *then*

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

Conjecture 5.2. *Let $p \equiv 3, 7 \pmod{20}$ be a prime, and hence $2p = x^2+5y^2$ for some integers x and y. If F_n is the Fibonacci sequence given by $F_0 = 0$, $F_1 = 1$ and $F_{n+1} = F_n + F_{n-1}$ $(n \geq 1)$, then*

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

REFERENCES

1. B.C. Berndt, R.J. Evans and K.S. Williams, *Gauss and Jacobi sums*, Wiley, New York, 1998.

2. L.E. Dickson, *History of the theory of numbers*, Vol. I, Chelsea, New York, 1952, 393–407.

3. K. Ireland and M. Rosen, *A classical introduction to modern number theory*, Springer, New York, 1982.

4. D.H. Lehmer, *An extended theory of Lucas' functions*, Ann. Math. **31** (1930), 419–448.

5. P. Ribenboim, *The book of prime number records*, 2nd ed., Springer, Berlin, 1989, pp. 44–50.

6. Z.H. Sun, *Combinatorial sum* $\sum_{k=0,k\equiv r \pmod m}^{n} \binom{n}{k}$ *and its applications in number theory* I, J. Nanjing Univ. Math. Biquarterly **9** (1992), 227–240. MR**94a**:11026.

7. ———, *Combinatorial sum* $\sum_{k=0,k\equiv r \pmod m}^{n} \binom{n}{k}$ *and its applications in number theory* II, J. Nanjing Univ. Math. Biquarterly **10** (1993), 105–118. MR**94j**:11021.

8. ———, *Combinatorial sum* $\sum_{k\equiv r \pmod m} \binom{n}{k}$ *and its applications in number theory* III, J. Nanjing Univ. Math. Biquarterly **12** (1995), 90–102. MR**96g**:11017.

9. ———, *On the theory of cubic residues and nonresidues*, Acta Arith. **84** (1998), 291–335. MR**99c**:11005.

10. ———, *Supplements to the theory of quartic residues*, Acta Arith. **97** (2001), 361–377. MR**2002c**:11007.

11. ———, *Notes on quartic residue symbol and rational reciprocity laws*, J. Nanjing Univ. Math. Biquarterly **9** (1992), 92–101. MR**94b**:11007.

12. ———, *Quartic residues and binary quadratic forms*, J. Number Theory, submitted.

13. ———, *Cubic and quartic congruences modulo a prime*, J. Number Theory **102** (2003), 41–89.

14. Z.H. Sun and Z.W. Sun, *Fibonacci numbers and Fermat's last theorem*, Acta Arith. **60** (1992), 371–388. MR**93e**:11025.

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