The Rocky Mountain Journal of Mathematics 33(2003), no.3, 1123-1145.

VALUES OF LUCAS SEQUENCES MODULO PRIMES

ZHI-HONG SUN

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

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 $u_{(p\pm1)/2}(a,b) \pmod p$, where $\{u_n(a,b)\}$ is the Lucas sequence given by $u_0(a,b)=0$, $u_1(a,b)=1$ and $u_{n+1}(a,b)=bu_n(a,b)-au_{n-1}(a,b)$ $(n \geqslant 1)$. In the case $a=-c^2$, a reciprocity law is established. As applications we obtain the criteria for $p \mid u_{\frac{p-1}{4}}(a,b)$ (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:

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

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

It is well known that

$$u_n(a,b)=\frac{1}{\sqrt{b^2-4a}}\left(\Big(\frac{b+\sqrt{b^2-4a}}{2}\Big)^n-\Big(\frac{b-\sqrt{b^2-4a}}{2}\Big)^n\right)\quad (b^2-4a\ne 0)\tag{1.3}$$

and

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

2000 *Mathematics Subject Classification*: 11B39,11B50,11A15.
Key words and phrases. Prime, Lucas sequence, reciprocity law.

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

$$u_{p-(\frac{b^2-4a}{p})}(a,b) \equiv 0 \pmod p \quad \text{and} \quad u_p(a,b) \equiv \Big(\frac{b^2-4a}{p}\Big) \pmod p,$$

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

Let $\{F_n\}$ be the Fibonacci sequence defined by $F_n = u_n(-1,1)$, and let $p \neq 5$ be an odd prime. In [14] we determined $F_{(p\pm 1)/2} \pmod p$ by proving that

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

and

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

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

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

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

and

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

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

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

and

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

In this paper we will determine $u_{(p\pm 1)/2}(a,b) \pmod p$ and $v_{(p\pm 1)/2}(a,b) \pmod p$ on the condition that $\left(\frac{4a-b^2}{p}\right) = 1$ or $\left(\frac{-a}{p}\right) = 1$. 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

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

and

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

where

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

Furthermore, if q is also an odd prime satisfying $q\nmid c$ and $p\equiv\pm q\pmod{(3-(-1)^b)(b^2+4c^2)}$, 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 $\left(\frac{4a-b^2}{p}\right)=1$. 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 $N\pi=\pi\overline{\pi}=a^2+b^2$. Here $\overline{\pi}$ 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 $\mathbb{Z}[i]$, then we may write $\pi=\pm\pi_1\pi_2\cdots\pi_r$, where $\pi_1,\cdots,\pi_r$ are primary primes. 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 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 $\mathbb{Z}[i]$, 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 $\mathbb{Z}[i]$, then

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

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

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

Now we can give

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

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

and

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

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 $\big(\frac{s+bi}{p}\big)_4=\big(\frac{s+bi}{p}\big)_4^{-1}=\pm1$, 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

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

Suppose $p = x^2 + y^2$ $(x, y \in \mathbb{Z})$ with $2|y$ 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

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

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

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

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,

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

and

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

Combining the above we obtain the result.

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

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

and

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

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

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

This together with Theorem 2.1 proves the corollary.

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

LEMMA 3.1. *Let p be an odd prime, $a, b \in \mathbb{Z}$, and $a' = (b^2 - 4a)/4$. Then*

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

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

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

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

Proof. Using induction one can easily prove the following known result (see [6]):

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

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

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

Thus,

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

and hence

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

That is,

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

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

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

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

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

Hence

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

The proof is now complete.

We are now ready to give

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

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

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

and

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

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

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

and

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

Proof. Let $a'\in\mathbb{Z}$ be such that $a'\equiv(b^2-4a)/4 \pmod p$. Then clearly $(2c)^2\equiv -4a\equiv 4a'-b^2 \pmod p$. Also,

$$u_n(a',b)\equiv u_n((b^2-4a)/4,b) \pmod p \quad\text{and}\quad v_n(a',b)\equiv v_n((b^2-4a)/4,b) \pmod p.$$

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 $4n+3$, $b,c\in\mathbb{Z}$, $p\nmid c$ and $\left(\frac{b^2+4c^2}{p}\right)=-1$. In [11] the author proved that

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

Now, it is an easy consequence of Theorem 3.1.

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

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

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

and

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

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

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

and

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

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, $b,c\in\mathbb{Z}$, $\gcd(b^2+4c^2,pq)=1$ and $p\equiv\pm q \pmod{(3-(-1)^b)(b^2+4c^2)}$. Then*

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

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

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

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 get

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

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 $b, c \in \mathbb{Z}$, $u_0 = 0$, $u_1 = 1$, $u_{n+1} = bu_n + c^2u_{n-1}$ $(n \geqslant 1)$, 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*

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

and

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

where

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

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

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

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

$$\left(\frac{b-2ci}{p}\right)_4 = \overline{\left(\frac{b+2ci}{p}\right)_4} = \left(\frac{b+2ci}{p}\right)_4^{-1} = \left(\frac{b+2ci}{p}\right)_4^{3} = \left(\frac{b+2ci}{p}\right)_4 (\frac{b^2+4c^2}{p}).$$

So

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

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 $p \equiv \pm q \pmod{(3-(-1)^b)(b^2+4c^2)}$, then $\left(\frac{b+2ci}{p}\right)_4 = \left(\frac{b+2ci}{q}\right)_4$ by Lemma 4.1. Since $\left(\frac{b+2ci}{p}\right)_4^2 = (\frac{b^2+4c^2}{p})$ and $\left(\frac{b+2ci}{q}\right)_4^2 = (\frac{b^2+4c^2}{q})$ 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 D.H.Lehmer. If $a, b \in \mathbb{Z}$, $(\frac{a}{p}) = 1$ and $p \nmid b^2 - 4a$, then

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

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

(3) Suppose that p is an odd prime and that a and b are integers. For the values of $u_{(p-(\frac{p}{3}))/3}(a,b) \pmod p$ 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

$$\delta_p \equiv \begin{cases} c_p(b^2+4c^2)^{-\frac{p-1}{4}} u_{\frac{p+(\frac{b^2+4c^2}{p})}{2}}(-c^2,b) \pmod p & \text{if } p\equiv 1 \pmod 4, \\ \frac{c_p}{b}(b^2+4c^2)^{\frac{p+1}{4}} u_{\frac{p+(\frac{b^2+4c^2}{p})}{2}}(-c^2,b) \pmod p & \text{if } p\equiv 3 \pmod 4. \end{cases} \tag{4.2}$$

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

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

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

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

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

and

$$u_{(p+(\frac{13}{p}))/2} \equiv \begin{cases} \delta_p\cdot 13^{\frac{p-1}{4}} \pmod p & \textit{if} \quad p\equiv 1 \pmod 4, \\ 3\delta_p\big(\frac{13}{p}\big)\cdot 13^{\frac{p-3}{4}} \pmod p & \textit{if} \quad p\equiv 3 \pmod 4, \end{cases}$$

where

$$\delta_p = \begin{cases} 1 & \textit{if } p\equiv \pm1,\pm5,\pm7,\pm9,\pm11,\pm23 \pmod{52}, \\ -1 & \textit{if } p\equiv \pm3,\pm15,\pm17,\pm19,\pm21,\pm25 \pmod{52}. \end{cases}$$

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

$$\delta_{53}=\delta_5=\delta_7=\delta_{43}=\delta_{11}=\delta_{23}=1 \quad \text{and} \quad \delta_{101}=\delta_{37}=\delta_{17}=\delta_{19}=\delta_{31}=\delta_{79}=-1.$$

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

$$Q_r(p) = \Big\{ k \mid \big(\frac{k+i}{p}\big)_4 = i^r,\ k \in S_p \Big\} \quad \text{for} \quad r = 0,1,2,3.$$

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 $k \in \mathbb{Z}$ 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

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

Note that $2^{(p-1)/2} \equiv (\frac{2}{p}) = (-1)^{[\frac{p+1}{4}]} \pmod p$ and $\big(\frac{k+i}{p}\big)_4^2 = (\frac{k^2+1}{p})$ 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, $a, b \in \mathbb{Z}$, $p \nmid a(b^2-4a)$ 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 $p \mid u_{\frac{p-1}{4}}(a,b)$ or $p \mid v_{\frac{p-1}{4}}(a,b)$.

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

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

(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

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

Hence, using Corollary 3.1 and the fact that

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

we obtain

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

So (i) is equivalent to (ii)

Since $\big(\frac{a}{p}\big) = \big(\frac{-a}{p}\big) = 1$, 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 $b^2+4 \neq p$. If $p = x^2+(b^2+4)y^2$ for some $x, y \in \mathbb{Z}$, 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 $(x/y)^2 \equiv -(b^2+4) \pmod p$. 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 $s \equiv \pm x/y \pmod p$ and so $(\frac{s}{p}) = (\frac{x}{p})(\frac{y}{p})$. Using the Jacobi symbol we see that

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

and

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

Hence, by Theorem 5.2 we have

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

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

$$p\mid u_{\frac{p-1}{4}}(-1,b)\iff (-1)^{\frac{p-1}{4}(\alpha+\beta)}=(-1)^{\alpha}\iff 4\mid x \text{ or } 4\mid y\iff 4\mid xy.$$

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 $x,y\in\mathbb{Z}$. Hence, it follows from Theorem 5.3 that $p\mid F_{(p-1)/4}$ 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 $16x^2+13y^2(x,y\in\mathbb{Z})$, then again $(\frac{13}{p})=\big(\frac{-13}{p}\big)=1$.

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

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

This is the result.

Remark 5.2 Let $p \equiv 1 \pmod 4$ be a prime, and $b \in \mathbb{Z}$ be with $(\frac{b^2+4}{p}) = 1$. Then $p \mid u_{\frac{p-1}{4}}(-1, b)$ if and only if p is 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 $\big(\frac{(3-(-1)^b)b+Bi}{A}\big)_4 = 1$. 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

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

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, pp. 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* $\sum_{\substack{k=0 \\ k\equiv r \pmod m}}^{n} \binom{n}{k}$ *and its applications in number theory I*, J. Nanjing Univ. Math. Biquarterly **9** (1992), 227-240, MR94a:11026.
7. ____, *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, MR94j: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, MR96g:11017.
9. ____, *On the theory of cubic residues and nonresidues*, Acta Arith. **84** (1998), 291-335, MR99c:11005.
10. ____, *Supplements to the theory of quartic residues*, Acta Arithmetica **97** (2001), 361-377.
11. ____, *Notes on quartic residue symbol and rational reciprocity laws*, J. Nanjing Univ. Math. Biquarterly **9** (1992), 92-101, MR94b: 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, MR93e:11025.