Journal of Number Theory 113(2005), no.1, 10-52.

QUARTIC RESIDUES AND BINARY QUADRATIC FORMS

ZHI-HONG SUN

Department of Mathematics, Huaiyin Teachers College,
Huaian, Jiangsu 223001, P.R. China
E-mail: hyzhsun@public.hy.js.cn
Homepage: http://www.hytc.cn/xsjl/szh

Communicated by David Goss

ABSTRACT. Let $p \equiv 1 \pmod 4$ be a prime, $m \in \mathbb{Z}$ and $p \nmid m$. In this paper we obtain a general criterion for m to be a quartic residue (mod p) in terms of appropriate binary quadratic forms. Let $d > 1$ be a squarefree integer such that $(\frac{d}{p}) = 1$, where $(\frac{d}{p})$ is the Legendre symbol, and let ε_d be the fundamental unit of the quadratic field $\mathbb{Q}(\sqrt{d})$. Since 1942 many mathematicians tried to characterize those primes p so that ε_d is a quadratic or quartic residue (mod p). In this paper we will completely solve these open problems by determining the value of $(u + v\sqrt{d})^{(p-(\frac{-1}{p}))/2} \pmod p$, where p is an odd prime, $u, v, d \in \mathbb{Z},\ v \neq 0,\ \gcd(u, v) = 1$ and $(\frac{-d}{p}) = 1$. As an application we also obtain a general criterion for $p \mid u_{(p-(\frac{-1}{p}))/4}(a, b)$, where $\{u_n(a, b)\}$ is the Lucas sequence defined by $u_0 = 0,\ u_1 = 1$ and $u_{n+1} = bu_n - au_{n-1}$ $(n \geq 1)$.

MSC: 11A15, 11E25, 11B39.

Keywords: Quartic residue; Quartic Jacobi symbol; Binary quadratic form.

1. Introduction.

Let $\mathbb{Z}$ be the set of integers, $i = \sqrt{-1}$ and $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$. We recall that $a + bi$ is primary when $b \equiv 0 \pmod 2$ and $a + b \equiv 1 \pmod 4$. If π or $-\pi$ is primary and $\alpha \in \mathbb{Z}[i]$, one can define the quartic Jacobi symbol $\left(\frac{\alpha}{\pi}\right)_4$ as in [S1].

For $a, b, c \in \mathbb{Z}$ denote the binary quadratic form $ax^2 + bxy + cy^2$ by (a, b, c), and denote the (proper) equivalent class that contains the form (a, b, c) by $[a, b, c]$. The discriminant of (a, b, c) is the integer $d = b^2 - 4ac$, only positive-definite forms are taken if $d < 0$. If an integer n is represented by (a, b, c), then n is also represented by any form in the class $[a, b, c]$. So we may say that n is represented by the class $[a, b, c]$. For $D \equiv 0, 1 \pmod 4$ let $H(D)$ be the form class group which consists of primitive, integral binary quadratic forms of discriminant D, and let $h(D) = |H(D)|$ be the corresponding class number.

Let $p \equiv 1 \pmod 4$ be a prime, and $m \in \mathbb{Z}$ with $p \nmid m$. The basic problem of quartic residues is to characterize those primes p for which m is a quartic residue (mod p). In

1828 Gauss proved the following Euler's conjecture: 2 is a quartic residue (mod p) if and only if $p = x^2 + 64y^2 (x, y \in \mathbb{Z})$. Here one may ask a natural question: how to generalize the result to an arbitrary integer m? When q is an odd prime different from p, the author proved in [S1] that $(-1)^{(q-1)/2}q$ is a quartic residue (mod p) if and only if p is represented by one of the fourth powers (under composition) of primitive quadratic forms of discriminant $-16q^2$. In Section 5 of this paper we will completely solve the above problem by proving the following result.

(1.1) Suppose that m' is the product of all the distinct odd prime divisors of $m \in \mathbb{Z}$, $m = 2^\alpha m_0 (2 \nmid m_0)$ and $m^* = 4m'/(4, m_0 - \alpha - 1)$, where (n_1, n_2) is the greatest common divisor of n_1 and n_2. If $p \equiv 1 \pmod 4$ is a prime such that $p \nmid m$, then m is a quartic residue (mod p) if and only if p is represented by one class in the set

$$G(m) = \Big\{ [a, 2b, c] \;\Big|\; \gcd(a, 2b, c) = 1,\ (2b)^2 - 4ac = -16{m^*}^2,\ a > 0,$$
$$a \equiv 1 \pmod 4,\ (a, m) = 1,\ \Big(\frac{(m+1)b - 2m^*(m-1)i}{a}\Big)_4 = 1 \Big\}.$$

Moreover, if m and $-m$ are nonsquare integers, then $G(m)$ is a subgroup of index 4 in the form class group $H(-16{m^*}^2)$.

Let $d > 1$ be a squarefree integer, and $\varepsilon_d = (m + n\sqrt{d})/2$ be the fundamental unit of the quadratic field $\mathbb{Q}(\sqrt{d})$. Suppose that $p \equiv 1 \pmod 4$ is a prime such that $(\frac{d}{p}) = 1$, where $(\frac{d}{p})$ is the Legendre symbol. One may ask a question: how to characterize those odd primes p so that ε_d is a quadratic or quartic residue (mod p)?

When the norm $N(\varepsilon_d) = (m^2 - dn^2)/4 = -1$, many mathematicians tried to characterize those primes p ($p \equiv 1 \pmod 4$, $(\frac{d}{p}) = 1$) for which ε_d is a quadratic residue (mod p). 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 $q = 5, 13, 37$ 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 [CI], [L], [LW1], [LW2], [FK], [H1], [H2], [HI] and [Lem, pp.168-170]. In Section 6 of this paper we will completely solve the problem by presenting the following general result.

(1.2) Suppose that $p \equiv 1 \pmod 4$ is a prime, $d, m, n \in \mathbb{Z}$, $m^2 - dn^2 = -4$ and $(\frac{d}{p}) = 1$. Then $(m + n\sqrt{d})/2$ is a quadratic residue (mod p) if and only if p is represented by one class in the set

$$S(m, n, d) = \Big\{ [a, 2b, c] \;\Big|\; [a, 2b, c] \in H(-4k^2 d),\ a \equiv 1 \pmod 4,\ \Big(\frac{bn - kmi}{a}\Big)_4 = 1 \Big\},$$

where

$$k = \begin{cases} 1 & \text{if } d \equiv 4 \pmod 8, \\ 2 & \text{if } d \equiv 0 \pmod 8 \text{ or } d \equiv 1 \pmod 2, \\ 4 & \text{if } d \equiv 2 \pmod 4. \end{cases}$$

Moreover, if $d \neq 1, 4$, then $S(m, n, d)$ is a subgroup of index 4 in $H(-4k^2d)$.

When the norm $N(\varepsilon_d) = 1$, how to characterize those primes p ($p \equiv 1 \pmod 4$, $(\frac{d}{p}) = 1$) in terms of binary quadratic forms so that ε_d is a quartic residue (mod p)? In 1974, using the cyclotomic numbers of order 12, E. Lehmer[L] proved that $\varepsilon_3 = 2 + \sqrt{3}$ is a quartic residue of a prime $p \equiv 1 \pmod{12}$ if and only if $p = x^2 + 192y^2$ for some integers x and y. She also conjectured that $\varepsilon_7 = 8 + 3\sqrt{7}$ is a quartic residue of p if and only if $p = x^2 + 448y^2$ for some integers x and y. In 1977, P.A. Leonard and K.S. Williams[LW1] proved Lehmer's conjecture and gave some additional special results. However, their method made them only succeed for the 21 imaginary bicyclic biquadratic fields having class number 1 and containing $\mathbb{Q}(\sqrt{-1})$, $\mathbb{Q}(\sqrt{-2})$ or $\mathbb{Q}(\sqrt{2})$ as a subfield. So they barely obtained partial results in the cases $d = 3, 7, 11, 19, 43, 67, 163, 6, 14, 22, 38, 86, 134$. In Section 8 we will completely solve the problem by proving the following general result.

(1.3) Suppose that $p \equiv 1 \pmod 4$ is a prime, $m, n, d \in \mathbb{Z}$, $m^2 - dn^2 = 4$, $p \nmid n$ and $(\frac{d}{p}) = 1$. Then $(m + n\sqrt{d})/2$ is a quartic residue (mod p) if and only if p is represented by one class in the set

$$N_0(m,n,d) = \Big\{ [a, 2b, c] \;\Big|\; b^2 - ac = -\delta(n,d)^2 d,\ a \equiv 1 \pmod 4,\ (a,b) = 1,\ \Big(\frac{\frac{bn}{(n,m-2)} - \delta(n,d)\frac{m-2}{(n,m-2)}i}{a}\Big)_4 = 1 \Big\},$$

where $\delta(n, d) \in \{1, 2, 4, 8\}$ is explicitly given by Table 4. Moreover, $N_0(m, n, d)$ is a subgroup of $H(-4\delta(n, d)^2 d)$.

Let $d > 1$ be a squarefree integer such that $N(\varepsilon_d) = 1$, and let $p \equiv 3 \pmod 4$ be a prime with $(\frac{-d}{p}) = 1$. In the book "Reciprocity laws: From Euler to Eisenstein" F. Lemmermeyer[Lem, p.418] proposed some open problems. The fourth problem is to determine $\varepsilon_d^{(p+1)/4} \pmod p$ in terms of appropriate binary quadratic forms. In Section 8 we will also solve this open problem.

For $a, b \in \mathbb{Z}$ the Lucas sequences $\{u_n(a, b)\}$ and $\{v_n(a, b)\}$ are defined below:

$$u_0(a,b) = 0,\ u_1(a,b) = 1,\ u_{n+1}(a,b) = bu_n(a,b) - au_{n-1}(a,b)\ (n \geq 1);$$
$$v_0(a,b) = 2,\ v_1(a,b) = b,\ v_{n+1}(a,b) = bv_n(a,b) - av_{n-1}(a,b)\ (n \geq 1).$$

Let p be an odd prime such that $(\frac{a}{p}) = (\frac{4a-b^2}{p}) = 1$. It is well known that (see [Le]) $p \mid u_{(p-(\frac{-1}{p}))/4}(a, b)$ or $p \mid v_{(p-(\frac{-1}{p}))/4}(a, b)$. How to characterize those odd primes p so that $p \mid u_{(p-(\frac{-1}{p}))/4}(a, b)$? Suppose that $p \equiv 1 \pmod 4$ is a prime and that $\{F_n\}$ ($F_n = u_n(-1, 1)$) is the Fibonacci sequence. In [SS] the author and his brother Zhi-Wei Sun showed that $p \mid F_{\frac{p-1}{4}}$ if and only if $p = x^2 + 5y^2 \neq 5$ with $x, y \in \mathbb{Z}$ and $4 \mid xy$. Let $P_n = u_n(-1, 2)$ be the Pell sequence. In 1974 E. Lehmer showed that $p \mid P_{\frac{p-1}{4}}$ if and only if $p = x^2 + 32y^2$ for some $x, y \in \mathbb{Z}$ (see [L],[S3]). Recently the author[S2] showed that $p \mid u_{\frac{p-1}{4}}(-1, 3)$ if and only if $p \neq 13$ is represented by $x^2 + 208y^2$ or $16x^2 + 13y^2$. In [S2] the author also proved the following result: Let $p \equiv 1 \pmod 4$ be

a prime, $2 \nmid b$, $b^2+4 \neq p$, and let p be represented by $x^2+16(b^2+4)y^2$ or $16x^2+(b^2+4)y^2$. Then $p \mid u_{\frac{p-1}{4}}(-1, b)$.

In Section 7 we will solve the above problem by proving the following general result.

(1.4) Let p be an odd prime, $a, b \in \mathbb{Z}$, $p \nmid a(b^2-4a)$, and let a' be the product of all the distinct odd prime divisors of a. If $a = 2^t a_0 (2 \nmid a_0)$,

$$\delta(a,b) = \begin{cases} \frac{8}{(8,b)} & \text{if } 2 \nmid t, \\ 4 & \text{if } 2 \mid t \text{ and } 2 \nmid b, \\ \frac{2}{(2, \frac{a+1}{2} \cdot \frac{b}{2} - 1)} & \text{if } 2 \nmid a \text{ and } 2 \mid b, \\ \frac{2}{(2, \frac{b}{2})} & \text{if } 2 \mid t,\ 2 \mid a \text{ and } 2 \mid b, \end{cases}$$

and $k = \delta(a,b)a'/(a',b)$, then $p \mid u_{(p-(\frac{-1}{p}))/4}(a,b)$ if and only if p is represented by one class in the set

$$G(a,b) = \Big\{ [A, 2B, C] \;\Big|\; [A, 2B, C] \in H(-4k^2(b^2-4a)),\ (A, 2a) = 1,\ \Big(\frac{kb+Bi}{A}\Big)_4 = 1 \Big\}.$$

Moreover, if a and $a(4a-b^2)$ are nonsquare integers, then $G(a,b)$ is a subgroup of index 4 in $H(-4k^2(b^2-4a))$.

Now we point out that (1.1)–(1.4) can be inferred from the following main result of the paper (see Theorem 4.1).

(1.5) Suppose that p is an odd prime, $u, v, d \in \mathbb{Z}$, $(u,v) = 1$, $v \neq 0$, $(\frac{-d}{p}) = 1$, $p \nmid u^2 - dv^2$ and $k = F(u,v,d)$, where $F(u,v,d)$ is defined by Definition 2.1. Then $\big(\frac{v\sqrt{d}+u}{v\sqrt{d}-u}\big)^{(p-(\frac{-1}{p}))/4} \equiv 1 \pmod{p}$ if and only if p is represented by one class in the set

$$G(u,v,d) = \Big\{ [a, 2b, c] \;\Big|\; [a, 2b, c] \in H(-4k^2 d),\ (a, 2(u^2-dv^2)) = 1,\ \Big(\frac{bv-kui}{a}\Big)_4 = 1 \Big\}.$$

Moreover, $G(u,v,d)$ is a subgroup of $H(-4k^2d)$; if u^2-dv^2 and $-d(u^2-dv^2)$ are nonsquare integers, then $|G(u,v,d)| = \frac{1}{4}h(-4k^2d)$.

Throughout this paper we use the following notation:

$\mathbb{N}$—the set of natural numbers, $\mathbb{Q}$—the set of rational numbers, $\mathbb{Z}[i] = \{a+bi \mid a, b \in \mathbb{Z}\}$, ε_d—the fundamental unit of the field $\mathbb{Q}(\sqrt{d})$, $|x|$—the absolute value of x, $[x]$—the greatest integer not exceeding x, $m \mid n$—m divides n, $m \nmid n$—m does not divide n, $p^\alpha \parallel n$—$p^\alpha \mid n$ but $p^{\alpha+1} \nmid n$, $\mathrm{ord}_p n$—the nonnegative integer s such that $p^s \parallel n$, (m,n)— the greatest common divisor of m and n, $\gcd(n_1, n_2, n_3)$—the greatest common divisor of n_1, n_2, n_3, $[n_1, \ldots, n_k]$—the least common multiple of $n_1, n_2, \ldots, n_k$, $\big(\frac{a}{m}\big)$—the quadratic Jacobi symbol, $\big(\frac{\alpha}{\pi}\big)_4$—the quartic Jacobi symbol, (a,b,c)—the quadratic form $ax^2+bxy+cy^2$, $(a,b,c) \sim (a',b',c')$— the form (a,b,c) is (properly) equivalent to the form (a',b',c'), $[a,b,c]$— the equivalent class that contains the form (a,b,c), $H(D)$—the form class group which consists of equivalence classes of primitive, integral binary quadratic forms of discriminant D, $h(D)$—the order of $H(D)$, $H_4(D)$—the subgroup of $H(D)$ consisting of the fourth powers of the classes in $H(D)$, Ker χ—the kernel of the group character χ.

2. Computing the quartic Jacobi symbol $\left(\frac{(ax+by)v+kuyi}{ax^2+2bxy+cy^2}\right)_4$.

If π or $-\pi$ is primary in $\mathbb{Z}[i]$, then we may write $\pi = \pm\pi_1\cdots\pi_r$, where $\pi_1,\ldots,\pi_r$ 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 (see [IR, p. 122]).

For later convenience we also define

$$\left(\frac{a+bi}{1}\right)_4 = \left(\frac{a+bi}{-1}\right)_4 = 1 \quad \text{for all} \quad a,b\in\mathbb{Z}.$$

According to [IR, pp. 122-123, 311], [BEW, pp. 242-243, 247] and [S1] 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 of $\mathbb{Z}[i]$, then

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

where $\overline{x}$ is the complex conjugate of x.

(2.3) 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:

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

(2.4) If $m,n\in\mathbb{Z}$, $2\nmid m$ and $(m,n)=1$, then $\left(\frac{n}{m}\right)_4 = 1$.

(2.5) If π or $-\pi$ is primary and $\alpha,\beta\in\mathbb{Z}[i]$, then $\left(\frac{\alpha\beta}{\pi}\right)_4 = \left(\frac{\alpha}{\pi}\right)_4\left(\frac{\beta}{\pi}\right)_4$.

(2.6) If π_1 and π_2 are primary and $\alpha\in\mathbb{Z}[i]$, then $\left(\frac{\alpha}{\pi_1\pi_2}\right)_4 = \left(\frac{\alpha}{\pi_1}\right)_4\left(\frac{\alpha}{\pi_2}\right)_4$.

Since $-1 = i^2$ and $2 = i^3(1+i)^2$, using (2.1) and (2.5) one can easily derive that

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

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

Using (2.3) and (2.7) one can also easily prove

(2.8) If $a,b,p\in\mathbb{Z}$ with $2\nmid ap$, $2\mid b$ and $(p,a^2+b^2)=1$, then

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

From [S4, Proposition 1] or [S1, Lemma 2.1] we have

(2.9) Let p be a positive odd number, $m,n\in\mathbb{Z}$ and $(m^2+n^2,p)=1$. Then

$$\left(\frac{m+ni}{p}\right)_4^2 = \left(\frac{m^2+n^2}{p}\right).$$

For later convenience we now introduce the following notation.

Definition 2.1. *Suppose* $u, v, d \in \mathbb{Z},\ dv(u^2 - dv^2) \neq 0$ *and* $(u, v) = 1$. *Let* $u^2 - dv^2 = (-1)^r 2^s W,\ W \equiv 1 \pmod 4$, *and let* w *be the product of all the distinct prime divisors of* W *(if* $W = 1$ *we set* $w = 1$*) . Then define*

$$f(u,v,d) = \begin{cases} \left[\frac{8}{(8,u)}, \frac{2}{(2,d)}\right] 2^{\mathrm{ord}_2 v} & \text{if } 2 \nmid s, \\ \frac{4}{(2, r+s/2)} 2^{\mathrm{ord}_2 v} & \text{if } 2 \mid s \text{ and } 2 \nmid u, \\ \frac{2}{(2,d)} & \text{if } 2 \mid s \text{ and } 4 \mid u, \\ \frac{2(2,d)}{(4, d+2r+s+2)} & \text{if } 2 \mid s \text{ and } 2 \parallel u \end{cases}$$

and

$$F(u,v,d) = \frac{w}{(u,w)} f(u,v,d).$$

We are now in a position to give the following key result, which plays a central role in the paper.

Theorem 2.1. *Suppose* $u, v, d \in \mathbb{Z},\ dv(u^2 - dv^2) \neq 0$ *and* $(u, v) = 1$. *If* $a, b, c, K, x, y \in \mathbb{Z},\ k = KF(u,v,d),\ b^2 - ac = -k^2 d$ *and* $(a(ax^2 + 2bxy + cy^2), 2Ky(u^2 - dv^2)) = 1$, *then*

$$\Big(\frac{(ax+by)v + kuyi}{ax^2 + 2bxy + cy^2}\Big)_4 = \Big(\frac{bv - kui}{a}\Big)_4.$$

Proof. Let $r, s, w, f(u,v,d)$ and $F(u,v,d)$ be given by Definition 2.1. Since $F(u,v,d) = \frac{w}{(u,w)} f(u,v,d),\ w \mid u^2 - dv^2$ and $(a(ax^2 + 2bxy + cy^2), 2Ky(u^2 - dv^2)) = 1$ we see that $(a(ax^2 + 2bxy + cy^2), F(u,v,d)) = 1$ and hence

$$(a(ax^2 + 2bxy + cy^2), 2ky(u^2 - dv^2)) = 1.$$

Now we claim that

$$\frac{w}{(u,w)} \,\Big|\, k,\ 2 \mid kd,\ 2 \,\Big|\, \frac{ku}{(k,v)} \quad \text{and} \quad 4 \,\Big|\, \frac{ksu}{(k,v)}. \tag{2.10}$$

Clearly $\frac{w}{(u,w)} \mid k$ since $\frac{w}{(u,w)} \mid F(u,v,d)$ and $F(u,v,d) \mid k$. From the definition of $f(u,v,d)$ we see that $\frac{2}{(2,d)} \mid f(u,v,d)$. Thus $\frac{2}{(2,d)} \mid k$ and hence $2 \mid kd$.

If $2 \mid u$, then clearly $2 \mid \frac{ku}{(k,v)}$. If $2 \nmid u$, by Definition 2.1 we have $\mathrm{ord}_2 k \geq \mathrm{ord}_2 f(u,v,d) \geq 1 + \mathrm{ord}_2 v$. Thus $2 \mid \frac{k}{(k,v)}$ and again $2 \mid \frac{ku}{(k,v)}$.

Now we show that $4 \mid \frac{ksu}{(k,v)}$. Since $2 \mid \frac{ku}{(k,v)}$ by the above, we see that the result is true when $2 \mid s$. Suppose $2 \nmid s$. By Definition 2.1 we have $\frac{8}{(8,u)} \cdot 2^{\mathrm{ord}_2 v} \mid f(u,v,d)$. Since $(8,u) \mid u$ and $f(u,v,d) \mid k$ we see that $8 \cdot 2^{\mathrm{ord}_2 v} \mid ku$. Thus $\frac{ku}{(k,v)} = \frac{ku}{(ku,v)} \equiv 0 \pmod 8$. Hence again $4 \mid \frac{ksu}{(k,v)}$. So (2.10) holds.

Let

$$S = \frac{ksu}{4(k,v)} + \frac{ku}{2(k,v)}\big(r + 1 + \frac{k^2 d}{2} + \mathrm{ord}_2 k - \mathrm{ord}_2 v\big).$$

We assert that $2 \mid S$. To prove this, we consider the following four cases.

CASE 1. $2 \nmid s$. In this case, by the above argument we know that $8 \mid \frac{ku}{(k,v)}$. Thus $2 \mid S$.

CASE 2. $2 \mid s$ and $2 \nmid u$. Since $2 \nmid u$ and $2 \mid \frac{ku}{(k,v)}$ we see that $2 \mid k$ and hence $4 \mid k^2 d$. Thus,

$$\begin{aligned} S &= \frac{ku}{2(k,v)}\big(\frac{s}{2} + r + 1 + \frac{k^2 d}{2} + \mathrm{ord}_2 k - \mathrm{ord}_2 v\big) \\ &\equiv \frac{k}{2(k,v)}(r + \frac{s}{2} + 1 + \mathrm{ord}_2 k - \mathrm{ord}_2 v) \pmod 2. \end{aligned}$$

Clearly $\mathrm{ord}_2 k \geq \mathrm{ord}_2 f(u,v,d) \geq 1 + \mathrm{ord}_2 v$. If $\mathrm{ord}_2 k \geq 2 + \mathrm{ord}_2 v$, then $4 \mid \frac{k}{(k,v)}$ and thus $2 \mid S$. If $\mathrm{ord}_2 k = 1 + \mathrm{ord}_2 v$, then $\mathrm{ord}_2 f(u,v,d) = 1 + \mathrm{ord}_2 v$ and hence $2 \mid (r + s/2)$. Thus,

$$S \equiv \frac{k}{2(k,v)}(r + \frac{s}{2} + 1 + \mathrm{ord}_2 k - \mathrm{ord}_2 v) \equiv r + \frac{s}{2} + 1 + 1 \equiv 0 \pmod 2.$$

CASE 3. $2 \mid s$ and $4 \mid u$. In this case, $2 \mid \frac{ku}{2(k,v)}$. Thus,

$$S = \frac{ku}{2(k,v)}\big(\frac{s}{2} + r + 1 + \frac{k^2 d}{2} + \mathrm{ord}_2 k - \mathrm{ord}_2 v\big) \equiv 0 \pmod 2.$$

CASE 4. $2 \mid s$ and $2 \parallel u$. Since $(u,v) = 1$ we see that $2 \nmid v$ and hence $2 \nmid (k,v)$. Thus,

$$\begin{aligned} S &= \frac{ku}{2(k,v)}\big(\frac{s}{2} + r + 1 + \frac{k^2 d}{2} + \mathrm{ord}_2 k - \mathrm{ord}_2 v\big) \\ &\equiv k(r + \frac{s}{2} + 1 + \frac{k^2 d}{2} + \mathrm{ord}_2 k) \pmod 2. \end{aligned}$$

Clearly $2 \mid S$ when $2 \mid k$. Now assume $2 \nmid k$. Then we have $f(u,v,d) = 1$ and so $d + 2r + s \equiv 2 \pmod 4$. Hence $S \equiv r + \frac{s}{2} + 1 + \frac{d}{2} \equiv 0 \pmod 2$.

Summarizing the four cases we get the assertion $2 \mid S$.

If $ky = 0$, then

$$(a(ax^2 + 2bxy + cy^2), 0) = (a(ax^2 + 2bxy + cy^2), 2ky(u^2 - dv^2)) = 1$$

and so $a(ax^2 + 2bxy + cy^2) = \pm 1$. Hence

$$\Big(\frac{(ax + by)v + kuyi}{ax^2 + 2bxy + cy^2}\Big)_4 = 1 = \Big(\frac{bv - kui}{a}\Big)_4.$$

So the result holds in this case.

Now assume $ky \neq 0$. Since $2 \nmid a(ax^2+2bxy+cy^2),\ 2 \mid kd$ and $a(ax^2+2bxy+cy^2) = (ax+by)^2+k^2dy^2$ we see that $2 \nmid ax+by$. Observing that $2 \mid \frac{ku}{(k,v)}$ and $(\frac{v}{(k,v)}, \frac{k}{(k,v)}u) = 1$ we also find $2 \nmid \frac{v}{(k,v)}$ and hence $2 \nmid \frac{v}{(v,ky)}$.

Let

$$A = (ax+by)\frac{v}{(v,ky)} \quad \text{and} \quad B = \frac{kuy}{(v,ky)} = \frac{ku}{(k,v)} \cdot \frac{y}{(v/(k,v),y)}.$$

By the above, it is clear that $A \equiv 1 \pmod 2$ and $B \equiv 0 \pmod 2$. Thus $(-1)^{(A+B-1)/2}(A+Bi)$ is primary in $\mathbb{Z}[i]$. Notice that $(ax^2+2bxy+cy^2, (v,ky)) = ((ax^2+2bxy+cy^2, ky), v) = 1$. So we have

$$\Big(\frac{(ax+by)v+kuyi}{ax^2+2bxy+cy^2}\Big)_4 = \Big(\frac{A+Bi}{ax^2+2bxy+cy^2}\Big)_4.$$

Since

$$\begin{aligned} a(ax^2+2bxy+cy^2)\frac{v^2}{(v,ky)^2} &= \big((ax+by)^2+k^2dy^2\big)\frac{v^2}{(v,ky)^2} \\ &= (ax+by)^2\frac{v^2}{(v,ky)^2} + \frac{k^2u^2y^2}{(v,ky)^2} + (dv^2-u^2)\frac{k^2y^2}{(v,ky)^2} \\ &= A^2+B^2+(dv^2-u^2)\frac{k^2y^2}{(v,ky)^2} \end{aligned}$$

and

$$(u,v) = (a(ax^2+2bxy+cy^2), 2ky(u^2-dv^2)) = 1$$

we see that

$$\begin{aligned} &(a(ax^2+2bxy+cy^2)v^2/(v,ky)^2,\ A^2+B^2) \\ &\quad = (a(ax^2+2bxy+cy^2)v^2/(v,ky)^2, (u^2-dv^2)k^2y^2/(v,ky)^2) = 1. \end{aligned}$$

Thus,

$$\Big(\frac{A+Bi}{a}\Big)_4\Big(\frac{A+Bi}{ax^2+2bxy+cy^2}\Big)_4\Big(\frac{A+Bi}{v^2/(v,ky)^2}\Big)_4 \neq 0.$$

As before we have $2 \mid kd,\ 2 \nmid ax+by$ and $2 \nmid \frac{v}{(v,ky)}$. So

$$\begin{aligned} a(ax^2+2bxy+cy^2)\frac{v^2}{(v,ky)^2} &= \big((ax+by)^2+k^2dy^2\big)\frac{v^2}{(v,ky)^2} \\ &\equiv 1+k^2dy^2 \equiv (-1)^{k^2dy^2/2} = (-1)^{k^2dy/2} \pmod 4. \end{aligned}$$

Hence , applying all the above and (2.1)-(2.3) we obtain

$$\begin{aligned}
&\Big(\frac{(ax+by)v+kuyi}{ax^2+2bxy+cy^2}\Big)_4=\Big(\frac{A+Bi}{ax^2+2bxy+cy^2}\Big)_4\\
&=\Big(\frac{A+Bi}{a(ax^2+2bxy+cy^2)v^2/(v,ky)^2}\Big)_4\Big(\frac{A+Bi}{av^2/(v,ky)^2}\Big)_4^{-1}\\
&=\Big(\frac{(-1)^{k^2dy/2}a(ax^2+2bxy+cy^2)v^2/(v,ky)^2}{A+Bi}\Big)_4\Big(\frac{A-Bi}{av^2/(v,ky)^2}\Big)_4\\
&=\Big(\frac{-1}{A+Bi}\Big)_4^{\frac{k^2dy}{2}}\Big(\frac{A^2+B^2+(dv^2-u^2)k^2y^2/(v,ky)^2}{A+Bi}\Big)_4\Big(\frac{A-Bi}{\frac{av^2}{(v,ky)^2}}\Big)_4\\
&=\Big(\frac{-1}{A+Bi}\Big)_4^{\frac{k^2dy}{2}}\Big(\frac{(dv^2-u^2)k^2y^2/(v,ky)^2}{A+Bi}\Big)_4\Big(\frac{A-Bi}{a}\Big)_4\Big(\frac{A-Bi}{\frac{v}{(v,ky)}}\Big)_4^2\\
&=\Big(\frac{-1}{A+Bi}\Big)_4^{\frac{k^2dy}{2}}\Big(\frac{(dv^2-u^2)\frac{k^2y^2}{(v,ky)^2}}{A+Bi}\Big)_4\Big(\frac{\frac{bvy}{(v,ky)}-\frac{kuy}{(v,ky)}i}{a}\Big)_4\Big(\frac{-Bi}{\frac{v}{(v,ky)}}\Big)_4^2\\
&=(-1)^{\frac{k^2dy}{2}\cdot\frac{B}{2}}\Big(\frac{(dv^2-u^2)k^2y^2/(v,ky)^2}{A+Bi}\Big)_4\Big(\frac{bv-kui}{a}\Big)_4\Big(\frac{-B^2}{v/(v,ky)}\Big)_4\\
&\quad\text{(note that }\Big(\frac{-1}{A+Bi}\Big)_4=(-1)^{\frac{B}{2}}\text{ and }(a,ky)=1)\\
&=(-1)^{\frac{k^2d}{2}\cdot\frac{B}{2}}\Big(\frac{(-1)^{r+1}2^sWk^2y^2/(v,ky)^2}{A+Bi}\Big)_4\Big(\frac{bv-kui}{a}\Big)_4\\
&\quad\text{(note that }(y-1)B/2\text{ is always even)}\\
&=(-1)^{(r+1+\frac{k^2d}{2})\frac{B}{2}}\Big(\frac{2^sk^2y^2/(v,ky)^2}{A+Bi}\Big)_4\Big(\frac{A+Bi}{W}\Big)_4\Big(\frac{bv-kui}{a}\Big)_4.
\end{aligned}$$

Suppose that p is a prime divisor of W. Then $p\mid w$. Since $\frac{w}{(u,w)}\mid k$ we see that $w\mid ku$ and hence $p\mid ku$. If $p\mid v$, we must have $p\mid u$ since $u^2=dv^2+(-1)^r2^sW$. But $(u,v)=1$, so $p\nmid v$. Hence $p\mid\frac{ku}{(k,v)}$ and therefore $p\mid B$. So we have

$$\Big(\frac{A+Bi}{W}\Big)_4=\prod_{p\mid W}\Big(\frac{A+Bi}{p}\Big)_4=\prod_{p\mid W}\Big(\frac{A}{p}\Big)_4=1.$$

Now let $n=\mathrm{ord}_2\frac{k}{(k,v)}$ and $t=\mathrm{ord}_2y$. Since $2\nmid\frac{v}{(k,v)}$ and $\frac{ky}{(v,ky)}=\frac{k}{(k,v)}\cdot\frac{y}{(v/(k,v),y)}$, we

see that $2^{n+t}\|\frac{ky}{(v,ky)}$. Assume $\frac{ky}{(v,ky)}=2^{n+t}M(2\nmid M)$. Then we have

$$\begin{aligned}\Big(\frac{2^sk^2y^2/(v,ky)^2}{A+Bi}\Big)_4&=\Big(\frac{2^{s+2n+2t}M^2}{A+Bi}\Big)_4=\Big(\frac{2}{A+Bi}\Big)_4^{s+2n+2t}\Big(\frac{A+Bi}{M^2}\Big)_4\\&=\Big(\frac{2}{(-1)^{(A+B-1)/2}(A+Bi)}\Big)_4^{s+2n+2t}\Big(\frac{A+Bi}{M}\Big)_4^2\\&=i^{-(-1)^{(A+B-1)/2}\frac{B}{2}(s+2n+2t)}\Big(\frac{A}{M}\Big)_4^2\\&\quad\text{(by (2.7) and the fact that } M\mid B)\\&=i^{-(A+B)\frac{B}{2}(s+2n+2t)}\\&\quad\text{(note that } (-1)^{(A+B-1)/2}\equiv A+B\pmod 4).\end{aligned}$$

Recall that $2\mid\frac{ku}{(k,v)}$, $2\nmid\frac{v}{(k,v)}$ and $2\nmid ax+by$. We find

$$\begin{aligned}(A+B)\frac{B}{2}&=\frac{(ax+by)v+kuy}{(v,ky)}\cdot\frac{kuy}{2(v,ky)}=\frac{kuy((ax+by)v+kuy)}{2(k,v)^2(v/(k,v),y)^2}\\&\equiv\frac{kuy((ax+by)v+kuy)}{2(k,v)^2}=\frac{kuvy(ax+by)}{2(k,v)^2}+2\big(\frac{kuy}{2(k,v)}\big)^2\\&\equiv\frac{kuy}{2(k,v)}\Big((ax+by)\frac{v}{(k,v)}+2\Big)\pmod 4\end{aligned}$$

and therefore

$$\begin{aligned}\Big(\frac{2^sk^2y^2/(v,ky)^2}{A+Bi}\Big)_4&=i^{-(s+2n+2t)(A+B)B/2}=i^{-(s+2n+2t)\frac{kuy}{2(k,v)}((ax+by)\frac{v}{(k,v)}+2)}\\&=i^{-s\frac{kuy}{2(k,v)}((ax+by)\frac{v}{(k,v)}+2)+2(n+t)\frac{kuy}{2(k,v)}}=i^{\frac{kuy}{2(k,v)}(2n+2s-s(ax+by)\frac{v}{(k,v)})}\\&\quad\text{(note that } 2s\equiv-2s\pmod 4\text{ and } 4\mid 2ty).\end{aligned}$$

As before we have $2\nmid\frac{v}{(k,v)}$. Thus

$$\frac{B}{2}=\frac{ku}{2(k,v)}\cdot\frac{y}{(v/(k,v),y)}\equiv\frac{kuy}{2(k,v)}\pmod 2$$

and so

$$(-1)^{(r+1+\frac{k^2d}{2})\frac{B}{2}}=(-1)^{(r+1+\frac{k^2d}{2})\frac{kuy}{2(k,v)}}=i^{2(r+1+\frac{k^2d}{2})\frac{kuy}{2(k,v)}}.$$

Now putting all the above together we get

$$\begin{aligned}&\Big(\frac{(ax+by)v+kuyi}{ax^2+2bxy+cy^2}\Big)_4\\&=(-1)^{(r+1+\frac{k^2d}{2})\frac{B}{2}}\Big(\frac{2^sk^2y^2/(v,ky)^2}{A+Bi}\Big)_4\Big(\frac{A+Bi}{W}\Big)_4\Big(\frac{bv-kui}{a}\Big)_4\\&=i^{2(r+1+\frac{k^2d}{2})\frac{kuy}{2(k,v)}}\cdot i^{\frac{kuy}{2(k,v)}(2n+2s-s(ax+by)\frac{v}{(k,v)})}\cdot 1\cdot\Big(\frac{bv-kui}{a}\Big)_4\\&=i^{\frac{kuy}{2(k,v)}\{2(r+s+1+\frac{k^2d}{2}+n)-s(ax+by)\frac{v}{(k,v)}\}}\Big(\frac{bv-kui}{a}\Big)_4.\end{aligned}$$

From the above we have $2\nmid ax+by$, $4\mid \frac{ksu}{(k,v)}$ and $2\nmid \frac{v}{(k,v)}$. So

$$i^{-\frac{kuy}{2(k,v)}(ax+by)s\frac{v}{(k,v)}}=(-1)^{-\frac{ksu}{4(k,v)}y(ax+by)\frac{v}{(k,v)}}=(-1)^{\frac{ksuy}{4(k,v)}}.$$

Note that $n=\mathrm{ord}_2k-\mathrm{ord}_2(k,v)=\mathrm{ord}_2k-\mathrm{ord}_2v$ since $2\nmid\frac{v}{(k,v)}$. By the above we get

$$\begin{aligned}\Big(\frac{(ax+by)v+kuyi}{ax^2+2bxy+cy^2}\Big)_4&=(-1)^{\{\frac{ksu}{4(k,v)}+\frac{ku}{2(k,v)}(r+1+\frac{k^2d}{2}+\mathrm{ord}_2k-\mathrm{ord}_2v)\}y}\Big(\frac{bv-kui}{a}\Big)_4\\&=(-1)^{Sy}\Big(\frac{bv-kui}{a}\Big)_4=\Big(\frac{bv-kui}{a}\Big)_4.\end{aligned}$$

We are done.

Remark 2.1 By the proof of Theorem 2.1, we have the following general result.

Suppose $u,v,d\in\mathbb{Z}$, $dv(u^2-dv^2)\neq 0$, $(u,v)=1$, and $u^2-dv^2=(-1)^r2^sW$ with $W\equiv 1\pmod 4$. Let w be the product of all the distinct prime divisors of W, and $a,b,c,k,x,y\in\mathbb{Z}$. If

$$(a(ax^2+2bxy+cy^2),2ky(u^2-dv^2))=1,\ b^2-ac=-k^2d,\ \frac{w}{(u,w)}\ \Big|\ k,\ 2\mid kd \text{ and } 2\ \Big|\ \frac{ku}{(k,v)},$$

then

$$\Big(\frac{(ax+by)v+kuyi}{ax^2+2bxy+cy^2}\Big)_4=i^{\frac{kmuy}{2(k,v)}}\Big(\frac{bv-kui}{a}\Big)_4,$$

where

$$m=2\big(r+s+1+\frac{k^2d}{2}+\mathrm{ord}_2k-\mathrm{ord}_2v\big)-s(ax+by)\frac{v}{(k,v)}.$$

Corollary 2.1. *Suppose $u,v,d\in\mathbb{Z}$, $dv(u^2-dv^2)\neq 0$ and $(u,v)=1$. If $a,b,c,a',b',c',K\in\mathbb{Z}$, $k=KF(u,v,d)$, $(a,2b,c)\sim(a',2b',c')$, $b^2-ac=-k^2d$ and $(aa',2K(u^2-dv^2))=1$, then*

$$\Big(\frac{b'v-kui}{a'}\Big)_4=\Big(\frac{bv-kui}{a}\Big)_4.$$

Proof. Since $(a,2b,c)\sim(a',2b',c')$, there are integers $\alpha,\beta,\gamma,\delta$ such that $\alpha\delta-\beta\gamma=1$ and

$$a(\alpha x+\beta y)^2+2b(\alpha x+\beta y)(\gamma x+\delta y)+c(\gamma x+\delta y)^2=a'x^2+2b'xy+c'y^2.$$

That is,

$$a'=a\alpha^2+2b\alpha\gamma+c\gamma^2,\ b'=a\alpha\beta+b(\alpha\delta+\beta\gamma)+c\gamma\delta,\ c'=a\beta^2+2b\beta\delta+c\delta^2. \tag{2.11}$$

Hence

$$\begin{aligned}b'\gamma&=a\alpha\beta\gamma+b\gamma(\alpha\delta+\beta\gamma)+c\gamma^2\delta\\&\equiv a\alpha\beta\gamma+b\beta\gamma^2+b\alpha\delta\gamma+\delta(-a\alpha^2-2b\alpha\gamma)\\&=a\alpha(\beta\gamma-\alpha\delta)+b\gamma(\beta\gamma+\alpha\delta-2\alpha\delta)\\&=(a\alpha+b\gamma)(\beta\gamma-\alpha\delta)=-(a\alpha+b\gamma)\ (\mathrm{mod}\ |a\alpha^2+2b\alpha\gamma+c\gamma^2|)\end{aligned}$$

and so

$$b'\frac{\gamma}{(a,\gamma)} \equiv -\frac{a}{(a,\gamma)}\alpha - b\frac{\gamma}{(a,\gamma)} \pmod{\frac{|a\alpha^2+2b\alpha\gamma+c\gamma^2|}{(a,\gamma)}}. \tag{2.12}$$

Let $a^* = a/(a,\gamma)$, $c^* = (a,\gamma)c$, $x = \alpha$ and $y = \gamma/(a,\gamma)$. By (2.11) and (2.12) we have

$$a^*x^2 + 2bxy + c^*y^2 = \frac{a\alpha^2+2b\alpha\gamma+c\gamma^2}{(a,\gamma)} = \frac{a'}{(a,\gamma)}$$

and

$$b'y \equiv -a^*x - by \pmod{|a^*x^2+2bxy+c^*y^2|}.$$

Since $(aa', 2K(u^2-dv^2)) = 1$ we see that $(a^*(a^*x^2+2bxy+c^*y^2), 2K(u^2-dv^2)) = 1$. Observe that $(\alpha,\gamma) = 1$ since $\alpha\delta - \beta\gamma = 1$. We find $(a^*x, y) = (\alpha a/(a,\gamma), \gamma/(a,\gamma)) = 1$. Hence

$$(a^*(a^*x^2+2bxy+c^*y^2), 2Ky(u^2-dv^2)) = 1.$$

Clearly we have $(2b)^2 - 4a^*c^* = (2b)^2 - 4ac = -4k^2d$. Thus, applying the above and Theorem 2.1 we get

$$\begin{aligned}\Big(\frac{b'v-kui}{a'/(a,\gamma)}\Big)_4 &= \Big(\frac{b'v-kui}{a^*x^2+2bxy+c^*y^2}\Big)_4 = \Big(\frac{-b'vy+kuyi}{a^*x^2+2bxy+c^*y^2}\Big)_4 \\ &= \Big(\frac{(a^*x+by)v+kuyi}{a^*x^2+2bxy+c^*y^2}\Big)_4 = \Big(\frac{bv-kui}{a^*}\Big)_4 = \Big(\frac{bv-kui}{a/(a,\gamma)}\Big)_4.\end{aligned}$$

Notice that $b' \equiv b\alpha\delta = b(1+\beta\gamma) \equiv b \pmod{(a,\gamma)}$. Then we see that

$$\Big(\frac{b'v-kui}{a'}\Big)_4 = \Big(\frac{b'v-kui}{(a,\gamma)}\Big)_4\Big(\frac{b'v-kui}{a'/(a,\gamma)}\Big)_4 = \Big(\frac{bv-kui}{(a,\gamma)}\Big)_4\Big(\frac{bv-kui}{a/(a,\gamma)}\Big)_4 = \Big(\frac{bv-kui}{a}\Big)_4.$$

This is the result.

3. The quartic characters on $H(-4k^2d)$.

In this section we use quartic Jacobi symbols to construct the quartic characters on the form class group $H(-4k^2d)$.

Lemma 3.1. *Suppose $a,b,c \in \mathbb{Z}$, $a \neq 0$, $\gcd(a,b,c) = 1$ and $M \in \mathbb{N}$. Then there is a primitive quadratic form $(a',b',c')(a',b',c' \in \mathbb{Z})$ such that $aa' > 0$, $(a',M) = 1$ and $(a',b',c') \sim (a,b,c)$.*

Proof. Gauss showed that there exist integers x, y such that $(x,y) = 1$ and $(ax^2 + bxy + cy^2, M) = 1$, see for example [Cox, Lemma 2.25]. Replacing x by $x + kM|y|$, where k is large enough, we get $a(ax^2+bxy+cy^2) > 0$. So there is an integer a' such that $aa' > 0$, $(a',M) = 1$ and a' is properly represented by (a,b,c). By a result of Gauss (see [Cox, Lemma 2.3]), a form properly represents a' if and only if it is properly equivalent to a form of the shape $(a',*,*)$. So the result follows.

Lemma 3.2. *Let (a_1, b_1, c_1) and (a_2, b_2, c_2) be two primitive, integral quadratic forms of the same discriminant d, $t = \gcd(a_1, a_2, \frac{b_1+b_2}{2})$, and let u, v, w be integers such that $a_1u + a_2v + \frac{b_1+b_2}{2}w = t$. If we set $a_3 = a_1a_2/t^2$, $b_3 = b_2 + 2a_2(\frac{b_1-b_2}{2}v - c_2w)/t$ and $c_3 = (b_3^2 - d)/(4a_3)$, then*

$$b_3 \equiv b_1 \pmod{2\frac{a_1}{t}}, \quad b_3 \equiv b_2 \pmod{2\frac{a_2}{t}} \quad \textit{and} \quad [a_1, b_1, c_1][a_2, b_2, c_2] = [a_3, b_3, c_3].$$

Proof. From [C, p.246] we know that $[a_1, b_1, c_1][a_2, b_2, c_2] = [a_3, b_3, c_3]$. Also, clearly $b_3 \equiv b_2 \pmod{2\frac{a_2}{t}}$. So it suffices to show that $b_3 \equiv b_1 \pmod{2\frac{a_1}{t}}$. Since $c_2 = (b_2^2 - d)/(4a_2) = (b_2^2 - b_1^2 + 4a_1c_1)/(4a_2)$, we see that

$$\begin{aligned} b_3 &= b_2 + \frac{2a_2}{t}\big(\frac{b_1 - b_2}{2}v - \frac{b_2^2 - b_1^2 + 4a_1c_1}{4a_2}w\big) \\ &= b_2 + \frac{a_2}{t}(b_1 - b_2)v + (b_1 - b_2)\frac{(b_1 + b_2)/2}{t}w - 2\frac{a_1}{t}c_1w \\ &\equiv b_2 + (b_1 - b_2)\big(\frac{a_2}{t}v + \frac{(b_1 + b_2)/2}{t}w\big) = b_2 + (b_1 - b_2)\big(1 - \frac{a_1}{t}u\big) \\ &\equiv b_2 + b_1 - b_2 = b_1 \pmod{2a_1/t}. \end{aligned}$$

This proves the lemma.

Lemma 3.3. *Let $(a_1, 2b_1, c_1)$ and $(a_2, 2b_2, c_2)$ be two primitive quadratic forms of discriminant $4d (d \in \mathbb{Z})$, and $2 \nmid a_1a_2$. If $(a_3, 2b_3, c_3)$ is the composition of $(a_1, 2b_1, c_1)$ and $(a_2, 2b_2, c_2)$ as defined in Lemma 3.2, and $u, v \in \mathbb{Z}$ with $(a_1, b_1^2u^2+v^2) = (a_2, b_2^2u^2+v^2) = 1$, then we have*

$$\Big(\frac{b_1u + vi}{a_1}\Big)_4\Big(\frac{b_2u + vi}{a_2}\Big)_4 = \Big(\frac{b_3u + vi}{a_3}\Big)_4.$$

Proof. Since $(a_1, b_1^2u^2+v^2) = (a_2, b_2^2u^2+v^2) = 1$ we see that $\big(\frac{b_1u+vi}{a_1}\big)_4\big(\frac{b_2u+vi}{a_2}\big)_4 \neq 0$. Let $t = \gcd(a_1, a_2, b_1 + b_2)$. From Lemma 3.2 we know that

$$a_3 = \frac{a_1}{t} \cdot \frac{a_2}{t} \quad \text{and} \quad 2b_3 \equiv 2b_s \pmod{2\frac{a_s}{t}} \quad (s = 1, 2).$$

Thus,

$$\begin{aligned} \Big(\frac{b_3u + vi}{a_3}\Big)_4 &= \Big(\frac{b_3u + vi}{a_1/t}\Big)_4\Big(\frac{b_3u + vi}{a_2/t}\Big)_4 = \Big(\frac{b_1u + vi}{a_1/t}\Big)_4\Big(\frac{b_2u + vi}{a_2/t}\Big)_4 \\ &= \Big(\frac{b_1u + vi}{a_1}\Big)_4\Big(\frac{b_1u + vi}{t}\Big)_4^{-1}\Big(\frac{b_2u + vi}{a_2}\Big)_4\Big(\frac{b_2u + vi}{t}\Big)_4^{-1} \\ &= \Big(\frac{b_1u + vi}{a_1}\Big)_4\Big(\frac{b_2u + vi}{a_2}\Big)_4\Big(\frac{b_1u - vi}{t}\Big)_4\Big(\frac{b_2u - vi}{t}\Big)_4. \end{aligned}$$

But, since $b_1 + b_2 \equiv 0 \pmod{t}$ we have

$$\begin{aligned} \Big(\frac{b_1u - vi}{t}\Big)_4\Big(\frac{b_2u - vi}{t}\Big)_4 &= \Big(\frac{(b_1u - vi)(b_2u - vi)}{t}\Big)_4 = \Big(\frac{b_1b_2u^2 - v^2 - (b_1 + b_2)uvi}{t}\Big)_4 \\ &= \Big(\frac{b_1b_2u^2 - v^2}{t}\Big)_4 = 1. \end{aligned}$$

Hence

$$\Big(\frac{b_3u+vi}{a_3}\Big)_4=\Big(\frac{b_1u+vi}{a_1}\Big)_4\Big(\frac{b_2u+vi}{a_2}\Big)_4.$$

This proves the lemma.

Lemma 3.4. *Suppose $D\in\mathbb{Z}-\{0\}$. Let G be a subgroup of $H(-16D)$, and let $G_1=\big\{[a,2b,c]\ \big|\ [a,2b,c]\in G,\ a\equiv 1\pmod 4\big\}$. Then*

(i) *G_1 is a subgroup of index 1 or 2 in G.*

(ii) *If $p\equiv 1\pmod 4$, then p is represented by one class in G if and only if p is represented by one class in G_1.*

Proof. For $[a,2b,c]\in H(-16D)$, it is known that (see [D] and [Cox, p.55]) $\chi([a,2b,c])=(-1)^{\frac{a-1}{2}}(2\nmid a)$ is a genus character on $H(-16D)$. So χ is also a character on G and hence G_1 is a subgroup of index 1 or 2 in G. This proves (i). Applying [Cox, Lemma 2.3] we get (ii) and hence the proof is complete.

Applying Chebotarev's density theorem to the field $\mathbb{Q}(\sqrt{u},\sqrt{v})$ one can easily derive the following result.

Lemma 3.5. *If u and v are nonsquare integers, then there are infinitely many primes q for which $(\frac{u}{q})=(\frac{v}{q})=-1$.*

We point out that Lemma 3.5 can also be proved by using Chinese remainder theorem and quadratic reciprocity law.

Now we are able to give

Theorem 3.1. *Suppose $u,v,d\in\mathbb{Z},\ dv(u^2-dv^2)\neq 0,\ (u,v)=1$, and $k=KF(u,v,d)$ with $K\in\mathbb{Z}$. For $[a,2b,c]\in H(-4k^2d)$ with $(a,2K(u^2-dv^2))=1$ define $\chi([a,2b,c])=\big(\frac{bv-kui}{a}\big)_4$. If $8\mid k^2d$, we also define $\chi'([a,2b,c])=\big(\frac{ku+bvi}{a}\big)_4$. Then χ and χ' (if $8\mid k^2d$) are quartic characters on $H(-4k^2d)$. Hence the kernels*

$$G(u,v,d,K)$$

$$=\mathrm{Ker}\ \chi=\Big\{[a,2b,c]\ \Big|\ [a,2b,c]\in H(-4k^2d),\ (a,2K(u^2-dv^2))=1,\ \Big(\frac{bv-kui}{a}\Big)_4=1\Big\},$$

$$G'(u,v,d,K)$$

$$=\mathrm{Ker}\ \chi'=\Big\{[a,2b,c]\ \Big|\ [a,2b,c]\in H(-4k^2d),\ (a,2K(u^2-dv^2))=1,\ \Big(\frac{ku+bvi}{a}\Big)_4=1\Big\}$$

are subgroups of $H(-4k^2d)$, and $H_4(-4k^2d)$ is a subgroup of $G(u,v,d,K)$ and $G'(u,v,d,K)$ (if $8\mid k^2d$) . Moreover, if u^2-dv^2 and $-d(u^2-dv^2)$ are nonsquare integers, then $|G(u,v,d,K)|=|G'(u,v,d,K)|=\frac{1}{4}h(-4k^2d)$.

Proof. From Corollary 2.1 and Lemma 3.1 we see that χ is well-defined, and clearly $\chi([1,0,k^2d])=1$. Thus, applying Lemma 3.3 we find that χ is a group homomorphism from $H(-4k^2d)$ to $\{\pm1,\pm i\}$. Hence χ is a character on $H(-4k^2d)$. If $8\mid k^2d$, define $\psi([a,2b,c])=(\frac{2}{|a|})$. Then clearly

$$\chi'([a,2b,c])=\Big(\frac{i}{a}\Big)_4\Big(\frac{bv-kui}{a}\Big)_4=\Big(\frac{2}{|a|}\Big)\chi([a,2b,c])$$

and so $\chi' = \chi\psi$. Using Corollary 2.1 and Lemma 3.2 one can show that ψ is a character of $H(-4k^2d)$. Actually it is well known that ψ is a genus character of $H(-4k^2d)$ (see [Cox, p.55] and [Bu]). So χ' is also a character on $H(-4k^2d)$. Therefore $H_4(-4k^2d) \subseteq$ Ker χ and $H_4(-4k^2d) \subseteq$ Ker χ' (if $8 \mid k^2d$).

From group theory we know that Ker χ and Ker χ' (if $8 \mid k^2d$) are subgroups on $H(-4k^2d)$. Now suppose that $u^2 - dv^2$ and $-d(u^2 - dv^2)$ are nonsquare integers. It follows from Lemma 3.5 that there are infinitely many primes q such that $\left(\frac{u^2-dv^2}{q}\right) = \left(\frac{-d(u^2-dv^2)}{q}\right) = -1$. Hence, there is an odd prime q satisfying $q \nmid k$ and $\left(\frac{u^2-dv^2}{q}\right) = -\left(\frac{-d}{q}\right) = -1$. For such a prime q, clearly $x^2 \equiv -d \pmod{q}$ for some $x \in \mathbb{Z}$ since $\left(\frac{-d}{q}\right) = 1$. On setting $b = kx$ and $c = k^2(x^2 + d)/q$, we find that

$$(q, b) = (q, 2k(u^2 - dv^2)) = 1,\ c \in \mathbb{Z} \quad \text{and} \quad (2b)^2 - 4cq = -4k^2d.$$

On the other hand, applying (2.9) we see that

$$\chi^2([q, 2b, c]) = \left(\frac{bv - kui}{q}\right)_4^2 = \left(\frac{b^2v^2 + k^2u^2}{q}\right) = \left(\frac{-k^2dv^2 + k^2u^2}{q}\right) = \left(\frac{u^2 - dv^2}{q}\right) = -1.$$

Hence $\chi([q, 2b, c]) = \pm i$. Since χ is a group character, we must have

$$\chi([q, 2b, c]^2) = -1,\ \chi([q, 2b, c]^3) = \mp i \quad \text{and} \quad \chi([q, 2b, c]^4) = 1.$$

Thus χ and so χ' (if $8 \mid k^2d$) are surjective homomorphisms. Therefore, $|Ker\chi| = |Ker\chi'| = \frac{1}{4}h(-4k^2d)$. This completes the proof.

Corollary 3.1. *Suppose that $d > 1$ is a nonsquare integer, and $u^2 - dv^2 = 1$ with $u, v \in \mathbb{Z}$ and $2 \nmid v$. For $[a, 2b, c] \in H(-16d)$ with $2 \nmid a$ define $\chi([a, 2b, c]) = \left(\frac{bv-2ui}{a}\right)_4$. Then χ is a quartic character on $H(-16d)$.*

Proof. Since $u^2 - dv^2 = 1$ and $2 \nmid v$, from Definition 2.1 we see that $r = s = 0,\ w = 1$ and $F(u, v, d) = f(u, v, d) = 1$ or 2. Now putting $k = 2$ in Theorem 3.1 yields the result.

4. Criteria for $\left(\frac{u+v\sqrt{d}}{u-v\sqrt{d}}\right)^{(p-(\frac{-1}{p}))/4} \pmod{p}$.

For positive odd number p let D_p be the set of those rational numbers whose denominator is prime to p. Following [S1] we define

$$Q_r(p) = \left\{k \;\middle|\; \left(\frac{k+i}{p}\right)_4 = i^r,\ k \in D_p\right\} \quad \text{for} \quad r = 0, 1, 2, 3. \tag{4.1}$$

Theorem 4.1. *Let p be an odd prime, $u, v, d \in \mathbb{Z},\ (u, v) = 1,\ v \neq 0,\ p \nmid d(u^2 - dv^2)$, $K \in \mathbb{Z},\ p \nmid K,\ k = KF(u, v, d)$ and $n = (p - (\frac{-1}{p}))/4$.*

(1) Assume that $p = ax^2 + 2bxy + cy^2 (a, b, c, x, y \in \mathbb{Z}),\ (a, 2Kp(u^2 - dv^2)) = 1$, $b^2 - ac = -k^2d$ and $j \in \{0, 1, 2, 3\}$. Then

$$\left(\frac{v\sqrt{d} + u}{v\sqrt{d} - u}\right)^n \equiv \left(\left(\frac{-1}{p}\right)\frac{ax + by}{kdy}\sqrt{d}\right)^j \pmod{p} \iff \left(\frac{bv - kui}{a}\right)_4 = i^j,$$

and if $8 \mid k^2d$, *then also*

$$\Big(\frac{u+v\sqrt{d}}{u-v\sqrt{d}}\Big)^n \equiv \Big(\Big(\frac{-1}{p}\Big)\frac{ax+by}{kdy}\sqrt{d}\Big)^j \pmod p \iff \Big(\frac{ku+bvi}{a}\Big)_4 = i^j.$$

(2) *Let* $(\frac{-d}{p}) = 1$, *and let* $G(u,v,d,K)$ *and* $G'(u,v,d,K)$ *be given in Theorem* 3.1. *Then* $\big(\frac{v\sqrt{d}+u}{v\sqrt{d}-u}\big)^n \equiv 1 \pmod p$ *if and only if* p *is represented by one class in* $G(u,v,d,K)$. *If* $8 \mid k^2d$, *then* $\big(\frac{u+v\sqrt{d}}{u-v\sqrt{d}}\big)^n \equiv 1 \pmod p$ *if and only if* p *is represented by one class in* $G'(u,v,d,K)$.

Proof. We show first that $p \nmid y$ and $(ax,y) = 1$. Indeed, if $p \mid y$, then $p \mid x$ since $p \nmid a$ and $p = ax^2 + 2bxy + cy^2$, so $p^2 \mid ax^2 + 2bxy + cy^2$, a contradiction. Hence $p \nmid y$, and $(ax,y) \mid p$ implies $(ax,y) = 1$. Since $ap = (ax+by)^2 + k^2dy^2$ and $p \nmid k$, we obtain

$$\Big(\frac{ax+by}{ky}\Big)^2 \equiv -d \pmod p \quad \text{and} \quad \Big(\Big(\frac{-1}{p}\Big)\frac{ax+by}{kdy}\sqrt{d}\Big)^2 \equiv -1 \pmod p.$$

If $p \mid u$, then clearly $p \nmid dv$ and $\big(\frac{v\sqrt{d}+u}{v\sqrt{d}-u}\big)^{(p-(\frac{-1}{p}))/4} \equiv 1 \pmod p$. Since $(a,2b,c)$ properly represents p, by [Cox, Lemma 2.3] we have $(a,2b,c) \sim (p,2b',c')$ for some $b',c' \in \mathbb{Z}$. Applying Corollary 2.1 we get

$$\Big(\frac{bv-kui}{a}\Big)_4 = \Big(\frac{b'v-kui}{p}\Big)_4 = \Big(\frac{b'v}{p}\Big)_4 = 1.$$

Now assume $p \nmid u$. By Theorem 2.1,

$$\Big(\frac{\frac{v}{u}\cdot\frac{ax+by}{ky}+i}{p}\Big)_4 = \Big(\frac{(ax+by)v+kuyi}{p}\Big)_4 = \Big(\frac{bv-kui}{a}\Big)_4.$$

Hence, if $\big(\frac{bv-kui}{a}\big)_4 = i^j$, then $\frac{v}{u}\cdot\frac{ax+by}{ky} \in Q_j(p)$ and so

$$\Big(\frac{v\sqrt{d}+u}{v\sqrt{d}-u}\Big)^n \equiv \Big(\frac{\frac{v}{u}\cdot\frac{ax+by}{ky}+\frac{ax+by}{kdy}\sqrt{d}}{\frac{v}{u}\cdot\frac{ax+by}{ky}-\frac{ax+by}{kdy}\sqrt{d}}\Big)^n \equiv \Big(\Big(\frac{-1}{p}\Big)\frac{ax+by}{kdy}\sqrt{d}\Big)^j \pmod p$$

by [S1, Theorem 2.3].

Assume now that $8 \mid k^2d$. Then $ap \equiv (ax+by)^2 \equiv 1 \pmod 8$, hence $a \equiv p \pmod 8$ and

$$i^{2n} = (-1)^n = \Big(\frac{2}{p}\Big) = \Big(\frac{2}{|a|}\Big) = (-1)^{\frac{a^2-1}{8}} = \Big(\frac{i}{a}\Big)_4.$$

If $\big(\frac{ku+bvi}{a}\big)_4 = i^j$, then

$$\Big(\frac{bv-kui}{a}\Big)_4 = \Big(\frac{ku+bvi}{a}\Big)_4\Big(\frac{i}{a}\Big)_4^{-1} = i^j\cdot i^{-2n} = i^{j-2n}$$

and therefore

$$\Big(\frac{u+v\sqrt{d}}{u-v\sqrt{d}}\Big)^n = (-1)^n\Big(\frac{v\sqrt{d}+u}{v\sqrt{d}-u}\Big)^n \equiv i^{2n}\Big(\Big(\frac{-1}{p}\Big)\frac{ax+by}{kdy}\sqrt{d}\Big)^{j-2n}$$
$$\equiv \Big(\Big(\frac{-1}{p}\Big)\frac{ax+by}{kdy}\sqrt{d}\Big)^j \pmod p.$$

If $(\frac{-d}{p}) = 1$, then p can be represented by some primitive form of discriminant $-4k^2d$, and therefore there exist $a, b, c \in \mathbb{Z}$ such that $\gcd(a, 2b, c) = 1$, $b^2 - ac = -k^2d$, $(a, 2Kp(u^2 - dv^2)) = 1$ and $p = ax^2 + 2bxy + cy^2$ for some $x, y \in \mathbb{Z}$. By the definition of $G(u, v, d, K)$, we have $[a, 2b, c] \in G(u, v, d, K)$ if and only if $\big(\frac{bv-kui}{a}\big)_4 = 1$. By (1), this is equivalent to $\big(\frac{v\sqrt{d}+u}{v\sqrt{d}-u}\big)^n \equiv 1 \pmod p$. So $\big(\frac{v\sqrt{d}+u}{v\sqrt{d}-u}\big)^n \equiv 1 \pmod p$ if and only if p is represented by one class in $G(u, v, d, K)$. The additional statement in the case $8 \mid k^2d$ can be proved in the same way.

Corollary 4.1. *Suppose that $p \equiv 1 \pmod 4$ is a prime, $u, v \in \mathbb{Z}$, $v \neq 0$, $(u, v) = 1$, $p \nmid u^2 - v^2$, and $k = KF(u, v, 1)$ with $K \in \mathbb{Z}$ and $p \nmid K$. Then $(v + u)/(v - u)$ is a quartic residue $\pmod p$ if and only if p can be represented by one class in $G(u, v, 1, K)$. Moreover, if $4 \mid k$, then $(u + v)/(u - v)$ is a quartic residue $\pmod p$ if and only if p is represented by one class in $G'(u, v, 1, K)$.*

Proof. Taking $d = 1$ in Theorem 4.1 and then applying Euler's criterion leads to the result.

Remark 4.1 For the class $[a, 2b, c]$ in $G(u, v, 1, K)$ or $G'(u, v, 1, K)$ we may further assume that $a > 0$ and $a \equiv 1 \pmod 4$ with no loss of generality.

Theorem 4.2. *Let p be an odd prime, $d \in \mathbb{Z}$, $d \not\equiv 0, 1 \pmod p$, $(\frac{-d}{p}) = 1$, $s(-d, p)^2 \equiv -d \pmod p$, $1 - d = (-1)^r 2^s W (W \equiv 1 \pmod 4)$, and let d_0 be the product of all the distinct odd prime divisors of $1 - d$. Then the following statements are equivalent:*

(1) $s(-d, p) \in Q_0(p)$.

(2) *There is an integer n such that $n^2 \equiv 1 - d \pmod p$ and $(\frac{n}{p}) = (\frac{n+1}{p})$.*

(3) *The congruence $x^4 + 2(d - 1)x^2 + d(d - 1) \equiv 0 \pmod p$ is solvable.*

(4) $-d \equiv (2x^2 - 1)/(x^2 - 1)^2 \pmod p$ *for some $x \in \mathbb{Z}$.*

(5) $\big(\frac{\sqrt{d}+1}{\sqrt{d}-1}\big)^{(p-(\frac{-1}{p}))/4} \equiv 1 \pmod p$.

(6) *p is represented by a primitive form $ax^2 + 2bxy + cy^2$ of discriminant $-4k^2d$ with the condition that $(a, 2(1 - d)) = 1$ and $\big(\frac{b-ki}{a}\big)_4 = 1$, where $k = 8d_0$ or $\frac{4d_0}{(2, r+s/2)}$ according as $2 \nmid s$ or $2 \mid s$.*

Proof. From [S1, Theorem 2.4] we know that (1) and (2) are equivalent, and from [S1, Theorem 2.3] we see that (1) is equivalent to (5) (see the proof of Theorem 4.1). Putting $u = v = K = 1$ in Theorem 4.1(ii) we find (5) and (6) are equivalent. Since $x^4 + 2(d-1)x^2 + d(d-1) = (x^2 - (1-d))^2 - (1-d)$, we see that $x^4 + 2(d-1)x^2 + d(d-1) \equiv 0 \pmod p$ is solvable if and only if there exists an integer n such that $n^2 \equiv 1 - d \pmod p$

and $x^2 - n^2 \equiv n \pmod p$ is solvable. This is equivalent to (2). So (3) is equivalent to (2). Observe that

$$\begin{aligned}&(s(-d,p)x)^4 + 2(d-1)(s(-d,p)x)^2 + d(d-1)\\ &\equiv d^2x^4 + 2d(1-d)x^2 + d(d-1) = -d\big(-d(x^2-1)^2 - 2x^2 + 1\big) \pmod p.\end{aligned}$$

We see that (3) is equivalent to (4). Hence the proof is complete.

Remark 4.2 Let p be an odd prime, $u, v, d \in \mathbb{Z}$, $(u,v) = 1$, $p \nmid uv(u^2 - dv^2)$, $(\frac{-d}{p}) = 1$ and $s(-d,p)^2 \equiv -d \pmod p$. Using Theorem 4.1 and the argument in the proof of Theorem 4.2 one can easily prove that the following statements are equivalent:

(1) $\frac{v}{u}s(-d,p) \in Q_0(p)$.

(2) $\big(\frac{v\sqrt{d}+u}{v\sqrt{d}-u}\big)^{(p-(\frac{-1}{p}))/4} \equiv 1 \pmod p$.

(3) p is represented by some class in $G(u,v,d,1)$.

(4) $x^4 - 2(u^2 - dv^2)x^2 - dv^2(u^2 - dv^2) \equiv 0 \pmod p$ is solvable.

(5) $\frac{u^2-dv^2}{u^2} \equiv \frac{x^4}{(x^2-1)^2} \pmod p$ for some integer x.

5. Criteria for m to be a quartic residue $\pmod p$.

In this section we present two criteria for m to be a quartic residue of p, where p is a prime of the form $4k+1$ and m is an integer not divisible by p.

Theorem 5.1. *Suppose that $m \in \mathbb{Z}$, $m = 2^\alpha m_0 (2 \nmid m_0)$, and $m^* = 4m'/(4, m_0 - 1 - \alpha)$, where m' is the product of all the distinct odd prime divisors of m. If $p \equiv 1 \pmod 4$ is a prime such that $p \nmid m$, then m is a quartic residue $\pmod p$ if and only if p can be represented by one class in the set*

$$\begin{aligned}G(m) = \Big\{&[a,2b,c] \;\Big|\; [a,2b,c] \in H(-16{m^*}^2),\ a \equiv 1 \pmod 4,\\ &(a,m) = 1,\ \Big(\frac{(m+1)b - 2m^*(m-1)i}{a}\Big)_4 = 1\Big\}.\end{aligned}$$

Moreover, $G(m)$ is a subgroup of $H(-16{m^*}^2)$; if m and $-m$ are nonsquare integers, then $|G(m)| = \frac{1}{4}h(-16{m^*}^2)$.

Proof. It's easy to check that $G(1) = \{[1,0,4]\}$ and $G(-1) = \{[1,0,16]\}$. Since

$$p \equiv 1 \pmod 4 \iff p = x^2 + 4y^2 \ (x, y \in \mathbb{Z})$$

and

$$p \equiv 1 \pmod 8 \iff p = x^2 + 16y^2 \ (x, y \in \mathbb{Z}),$$

we see that the result holds for $m = \pm 1$.

Now assume $m \neq \pm 1$. Let us consider the following three cases.

CASE 1. $m \equiv 0 \pmod 2$. Let $u = m - 1$ and $v = m + 1$. From Definition 2.1 one can easily verify that $f(u,v,1) = 8/(4, m_0 - 1 - \alpha)$ and $F(u,v,1) = 2m^*$. Now taking $K = 1$ in Corollary 4.1 and then applying Theorem 3.1 and Remark 4.1 yields the result.

CASE 2. $m \equiv 1 \pmod 4$. In this case, $m_0 = m,\ \alpha = 0$, thus $m^* = 4m'/(4, m_0 - 1 - \alpha) = 4m'/(4, m-1) = m'$. On setting $u = (m-1)/2$ and $v = (m+1)/2$, from Definition 2.1 we see that

$$f(u,v,1) = 2 \quad \text{and} \quad F(u,v,1) = \frac{m'}{((m-1)/2, m')} f(u,v,1) = 2m' = 2m^*.$$

Thus applying Corollary 4.1, Theorem 3.1 and Remark 4.1 we get the result.

CASE 3. $m \equiv 3 \pmod 4$. In this case, $m_0 = m,\ \alpha = 0$, thus $m^* = 4m'/(4, m_0 - 1 - \alpha) = 4m'/(4, m-1) = 2m'$. Set $u = (m+1)/2$ and $v = (m-1)/2$. By Definition 2.1 we have $f(u,v,1) = 2$ and $F(u,v,1) = 2m' = m^*$. Hence taking $K = 2$ in Corollary 4.1 and applying Theorem 3.1 and Remark 4.1 we see that m is a quartic residue (mod p) if and only if p can be represented by some class in the set

$$G'(m) = \Big\{ [a,2b,c] \;\Big|\; \gcd(a,2b,c) = 1,\ (2b)^2 - 4ac = -64{m'}^2,\ a > 0,$$
$$a \equiv 1 \pmod 4,\ (a,m) = 1,\ \Big(\frac{2m^* \cdot \frac{m+1}{2} + \frac{m-1}{2} bi}{a}\Big)_4 = 1 \Big\}.$$

To see the result $G'(m) = G(m)$, we note that

$$\begin{aligned}
&\Big(\frac{(m+1)b - 2m^*(m-1)i}{a}\Big)_4 \Big(\frac{2m^* \cdot \frac{m+1}{2} - \frac{m-1}{2} bi}{a}\Big)_4 \\
&= \Big(\frac{((m+1)b - 2m^*(m-1)i)(m^*(m+1) - \frac{m-1}{2} bi)}{a}\Big)_4 \\
&= \Big(\frac{((m+1)^2 - (m-1)^2) m^* b - \frac{m^2-1}{2}(b^2 + 4{m^*}^2) i}{a}\Big)_4 \\
&= \Big(\frac{4mm^*b - \frac{m^2-1}{2} aci}{a}\Big)_4 = \Big(\frac{4mm^*b}{a}\Big)_4 = 1
\end{aligned}$$

and therefore

$$\Big(\frac{(m+1)b - 2m^*(m-1)i}{a}\Big)_4 = \Big(\frac{2m^* \cdot \frac{m+1}{2} - \frac{m-1}{2} bi}{a}\Big)_4^{-1} = \Big(\frac{2m^* \cdot \frac{m+1}{2} + \frac{m-1}{2} bi}{a}\Big)_4.$$

Summarizing the above we get the assertion.

Corollary 5.1. *Suppose that $m \in \mathbb{Z}$, $m = 2^\alpha m_0 (2 \nmid m_0)$, and $m^* = 4m'/(4, m_0 - 1 - \alpha)$, where m' is the product of all the distinct odd prime divisors of m. If $p \equiv 1 \pmod 4$ is a prime such that $p \nmid m$, and if p is represented by one of the fourth powers (undercomposition) of primitive quadratic forms of discriminant $-16{m^*}^2$, then m is a quartic residue (mod p).*

Proof. Let $[a,2b,c] \in H(-16{m^*}^2)$ with $(a, 2m) = 1$. Then clearly $(a, 2b) = 1$ since $b^2 - ac = -4{m^*}^2$. Observing that

$$\begin{aligned}
((m+1)b)^2 + (2m^*(m-1))^2 &= (m+1)^2(ac - 4{m^*}^2) + 4{m^*}^2(m-1)^2 \\
&\equiv 4{m^*}^2((m-1)^2 - (m+1)^2) = -16mm^{*2} \pmod{|a|}
\end{aligned}$$

we find $(a,((m+1)b)^2+(2m^*(m-1))^2)=1$ and hence $\left(\frac{(m+1)b-2m^*(m-1)i}{a}\right)_4\neq 0$.

Now suppose $[a,2b,c]^s=[a_s,2b_s,c_s]$ $(s=1,2,3,4)$. Then we may take $a_2=a^2$ and hence $a_4=a_2^2=a^4$ by Lemma 3.2. Thus $(a_4,2m)=1$ and

$$\Big(\frac{(m+1)b_4-2m^*(m-1)i}{a_4}\Big)_4=\Big(\frac{(m+1)b_4-2m^*(m-1)i}{a}\Big)_4^4=1.$$

Hence $[a_4,2b_4,c_4]=[a,2b,c]^4\in G(m)$, where $G(m)$ is given in Theorem 5.1.

By Lemma 3.1 and the assumption, there exists a primitive quadratic form $(a,2b,c)$ of discriminant $-16m^{*2}$ such that $(a,2m)=1$ and that p is represented by the class $[a,2b,c]^4$. Applying the above we see that $[a,2b,c]^4\in G(m)$. So m is a quartic residue (mod p) by Theorem 5.1

Corollary 5.2. *Let $m\in\{\pm2,\pm3,\dots,\pm10\}$. If $p\equiv 1 \pmod 4$ is a prime such that $p\nmid m$, then m is a quartic residue* (mod p) *if and only if p is represented by one of the corresponding quadratic forms in Table* 1.

Table 1.

m	*Corresponding quadratic forms*
$\pm$ 2	x^2+64y^2
3	$x^2+144y^2,\ 13x^2+10xy+13y^2$
$-$ 3	x^2+36y^2
4	x^2+16y^2
$-$ 4	x^2+4y^2
5	x^2+100y^2
$-$ 5	$x^2+400y^2,\ 16x^2+16xy+29y^2$
6	$x^2+576y^2,\ 25x^2+14xy+25y^2,\ 5x^2\pm4xy+116y^2$
$-$ 6	$x^2+576y^2,\ 25x^2+14xy+25y^2,\ 20x^2\pm4xy+29y^2$
7	$x^2+784y^2,\ 16x^2+49y^2,\ 29x^2\pm24xy+32y^2$
$-$ 7	$x^2+196y^2,\ 4x^2+49y^2$
$\pm$ 8	x^2+64y^2
9	$x^2+36y^2,\ 4x^2+9y^2$
$-$ 9	$x^2+144y^2,\ 9x^2+16y^2, 5x^2\pm2xy+29y^2$
10	$x^2+1600y^2,\ 41x^2+18xy+41y^2,\ 37x^2\pm36xy+52y^2$
$-$ 10	$x^2+1600y^2,\ 41x^2+18xy+41y^2,\ 13x^2\pm10xy+125y^2$

Corollary 5.2 can be easily proved by Theorem 5.1, the theory of reduced forms and some computations.

Now we give another criterion for m to be a quartic residue (mod p), which extends Theorem 2.2 of [S1].

For positive odd number n let $Q_r(n)(r=0,1,2,3)$ be defined by (4.1). Then we have

Theorem 5.2. *Let $p\equiv 1 \pmod 4$ be a prime, and $p=a^2+b^2(a,b\in\mathbb{Z})$ with $2\mid b$ and $4\mid a+b-1$. If $m\in\mathbb{Z}$, $p\nmid m$, $m=(-1)^r2^sm_1$, $m_1\equiv 1 \pmod 4$, and $k\in\{0,1,2,3\}$, then $m^{(p-1)/4}\equiv(b/a)^k \pmod p$ if and only if $a/b\in Q_j(M)$, where M is the product of*

all odd primes dividing m but not b, and $j \in \{0,1,2,3\}$ is determined by the congruence $j \equiv k-(2r-s)b/2 \pmod 4$.

Proof. Set $\pi = a+bi$. Then clearly $p = \pi\bar{\pi}$ and $b/a \equiv i \pmod{\pi}$ since $(a,b)=1$. Note that π is primary. Applying (2.3), (2.5) and (2.7) we see that

$$\begin{aligned}
&m^{\frac{p-1}{4}} \equiv (b/a)^k \pmod p\\
&\iff m^{\frac{p-1}{4}} \equiv (b/a)^k \equiv i^k \pmod{\pi} \iff \Big(\frac{(-1)^r 2^s m_1}{\pi}\Big)_4 = \Big(\frac{m}{\pi}\Big)_4 = i^k\\
&\iff \Big(\frac{-1}{\pi}\Big)_4^r \Big(\frac{2}{\pi}\Big)_4^s \Big(\frac{m_1}{\pi}\Big)_4 = i^k \iff (-1)^{\frac{rb}{2}} i^{-\frac{sb}{2}} \Big(\frac{\pi}{m_1}\Big)_4 = i^k\\
&\iff \Big(\frac{\pi}{m_1}\Big)_4 = i^{k-(2r-s)b/2} = i^j.
\end{aligned}$$

Let q be any odd prime divisor of m_1. If $q \mid b$, then $\big(\frac{a+bi}{q}\big)_4 = \big(\frac{a}{q}\big)_4 = 1$ since $(a,b)=1$. Thus,

$$\Big(\frac{\pi}{m_1}\Big)_4 = \prod_{q\mid m_1} \Big(\frac{a+bi}{q}\Big)_4 = \prod_{q\mid m_1, q\nmid b} \Big(\frac{a+bi}{q}\Big)_4 = \Big(\frac{a+bi}{M}\Big)_4 = \Big(\frac{a/b+i}{M}\Big)_4.$$

Hence

$$m^{\frac{p-1}{4}} \equiv \Big(\frac{b}{a}\Big)^k \pmod p \iff \Big(\frac{a/b+i}{M}\Big)_4 = i^j \iff \frac{a}{b} \in Q_j(M).$$

This proves the theorem.

6. Criteria for ε_d to be a quadratic residue (mod p)**.**

Suppose that $d>1$ is a squarefree integer, and $\varepsilon_d = (m+n\sqrt{d})/2$ denotes the fundamental unit in the quadratic field $\mathbb{Q}(\sqrt{d})$. Then clearly $m^2-dn^2 = 4$ or -4 according as $N(\varepsilon_d)=1$ or -1, where $N(\varepsilon_d)$ is the norm of ε_d.

Lemma 6.1. *Suppose $d,m,n \in \mathbb{Z}$ and $m^2-dn^2=-4$. Then $(m,n)=1$ or 2, and $n/(m,n)$ is odd.*

Proof. Since $(m,n)\mid m$ and $(m,n)\mid n$ we find $(m,n)^2 \mid m^2-dn^2$. That is, $(m,n)^2 \mid 4$. Hence $(m,n)=1$ or 2. If $(m,n)=1$, then $n/(m,n)=n$ and clearly n is odd since $m^2-dn^2=-4$. If $(m,n)=2$, then $n/(m,n)=n/2$. When $\frac{n}{2}$ is even, we have $2 \nmid \frac{m}{2}$ and so $(\frac{m}{2})^2+1 \equiv 2 \pmod 4$. On the other hand, $(\frac{m}{2})^2+1 = d(\frac{n}{2})^2 \equiv 0 \pmod 4$. This is a contradiction. So $n/2$ must be odd and hence the lemma is proved.

If $m,n,d \in \mathbb{Z}$ and $m^2-dn^2=-4$, one can easily show that

$$\frac{m}{(m,n)} = \begin{cases} m \equiv 1+(-1)^{\frac{d}{4}} \pmod 4 & \text{if } 4 \mid d,\\ m \equiv 1 \pmod 2 & \text{if } 2 \nmid dm,\\ \frac{m}{2} \equiv 0 \pmod 2 & \text{if } 2 \nmid d \text{ and } 2 \mid m,\\ \frac{m}{2} \equiv 1 \pmod 2 & \text{if } d \equiv 2 \pmod 4. \end{cases} \tag{6.1}$$

From (6.1), Definition 2.1 and Lemma 6.1 one can deduce

Lemma 6.2. *Suppose* $d, m, n \in \mathbb{Z},\ m^2 - dn^2 = -4,\ u = m/(m,n)$ *and* $v = n/(m,n)$. *Then*

$$F(u,v,d) = f(u,v,d) = \begin{cases} 1 & \text{if } d \equiv 4 \pmod 8, \\ 2 & \text{if } 8 \mid d \text{ or } 2 \nmid d, \\ 4 & \text{if } d \equiv 2 \pmod 4. \end{cases}$$

Now we are in a position to give

Theorem 6.1. *Suppose that* p *is an odd prime,* $d, m, n \in \mathbb{Z},\ m^2 - dn^2 = -4$, $(\frac{-d}{p}) = 1$, *and* $p = ax^2 + 2bxy + cy^2 (a, b, c, x, y \in \mathbb{Z})$ *with* $p \nmid a, 2 \nmid a$ *and* $b^2 - ac = -k^2 d$, *where* k *is given by*

$$k = \begin{cases} 1 & \text{if } d \equiv 4 \pmod 8, \\ 2 & \text{if } 8 \mid d \text{ or } 2 \nmid d, \\ 4 & \text{if } d \equiv 2 \pmod 4. \end{cases} \tag{6.2}$$

If $\left(\frac{bn-kmi}{a}\right)_4 = i^j$, *then we have*

$$\left(\frac{m+n\sqrt{d}}{2}\right)^{\frac{p-(\frac{-1}{p})}{2}} \equiv \left(\left(\frac{-1}{p}\right)\frac{ax+by}{kdy}\sqrt{d}\right)^j \pmod p.$$

Proof. Let $u = m/(m,n)$ and $v = n/(m,n)$. Then $v \neq 0,\ (u,v) = 1$ and $p \nmid u^2 - dv^2$. Since

$$\left(\frac{v\sqrt{d}+u}{v\sqrt{d}-u}\right)^{\frac{p-(\frac{-1}{p})}{4}} = \left(\frac{n\sqrt{d}+m}{n\sqrt{d}-m}\right)^{\frac{p-(\frac{-1}{p})}{4}} = \left(\frac{m+n\sqrt{d}}{2}\right)^{\frac{p-(\frac{-1}{p})}{2}}$$

and $k = F(u,v,d)$ by Lemma 6.2, putting $K = 1$ in Theorem 4.1 we obtain the result.

As examples, taking $m = 1, 3$ in Theorem 6.1 one can easily obtain the following results:

(6.3) If p is a prime such that $p \equiv 3, 7 \pmod{20}$ and $p \neq 3$, then $p = 3x^2 - 2xy + 7y^2$ (i.e. $3p = (3x-y)^2 + 20y^2$) for some $x, y \in \mathbb{Z}$ and

$$\left(\frac{1+\sqrt{5}}{2}\right)^{\frac{p+1}{2}} \equiv -\frac{3x-y}{10y}\sqrt{5} \pmod p.$$

(6.4) If p is a prime with $p \equiv 7, 11, 15, 19, 31, 47 \pmod{52}$ and $p \neq 7$, then $p = 7x^2 + 4xy + 8y^2$ (i.e. $7p = (7x+2y)^2 + 52y^2$) for some $x, y \in \mathbb{Z}$ and

$$\left(\frac{3+\sqrt{13}}{2}\right)^{\frac{p+1}{2}} \equiv -\frac{7x+2y}{26y}\sqrt{13} \pmod p.$$

From Theorem 6.1 we have

Theorem 6.2. *Suppose that p is an odd prime, $d, m, n \in \mathbb{Z}$, $m^2 - dn^2 = -4$ and $(\frac{-d}{p}) = 1$. Then $(\frac{m+n\sqrt{d}}{2})^{(p-(\frac{-1}{p}))/2} \equiv 1 \pmod{p}$ if and only if p can be represented by one class in the set*

$$S(m,n,d) = \Big\{ [a,2b,c] \;\Big|\; [a,2b,c] \in H(-4k^2d),\ a \equiv 1 \pmod 4,\ \Big(\frac{bn-kmi}{a}\Big)_4 = 1 \Big\},$$

where k is given by (6.2). Moreover, if $d \neq 1, 4$, then $S(m,n,d)$ is a subgroup of index 4 in $H(-4k^2d)$.

Proof. Let $u = m/(m,n)$ and $v = n/(m,n)$. Then clearly $(u,v) = 1$, $v \neq 0$, $u^2 - dv^2 = -(2/(m,n))^2 \not\equiv 0 \pmod p$ and

$$\frac{v\sqrt{d}+u}{v\sqrt{d}-u} = \frac{n\sqrt{d}+m}{n\sqrt{d}-m} = \frac{(m+n\sqrt{d})^2}{dn^2-m^2} = \Big(\frac{m+n\sqrt{d}}{2}\Big)^2.$$

From Lemma 6.2 we know that $k = F(u,v,d)$. Thus, from Theorem 4.1 we see that $(\frac{m+n\sqrt{d}}{2})^{(p-(\frac{-1}{p})/2} = (\frac{v\sqrt{d}+u}{v\sqrt{d}-u})^{(p-(\frac{-1}{p}))/4} \equiv 1 \pmod p$ if and only if p is represented by one class in the set

$$G(u,v,d,1) = \Big\{ [a,2b,c] \;\Big|\; [a,2b,c] \in H(-4k^2d),\ 2 \nmid a,\ \Big(\frac{bv-kui}{a}\Big)_4 = 1 \Big\}.$$

For $[a,2b,c] \in G(u,v,d,1)$ we may suppose $a > 0$ by Lemma 3.1 and the theory of reduced forms. Notice that

$$\begin{aligned}\Big(\frac{bv-kui}{a}\Big)_4^2 = \Big(\frac{bn-kmi}{a}\Big)_4^2 = \Big(\frac{b^2n^2+k^2m^2}{a}\Big) = \Big(\frac{(ac-k^2d)n^2+k^2m^2}{a}\Big) \quad \text{(by (2.9))}\\ = \Big(\frac{k^2(m^2-dn^2)}{a}\Big) = \Big(\frac{-4k^2}{a}\Big) = \Big(\frac{-1}{a}\Big) = (-1)^{\frac{a-1}{2}}.\end{aligned}$$

We find that $\big(\frac{bv-kui}{a}\big)_4 = 1$ implies $a \equiv 1 \pmod 4$. Hence $S(m,n,d) = G(u,v,d,1)$. Thus we see that $(\frac{m+n\sqrt{d}}{2})^{(p-(\frac{-1}{p}))/2} \equiv 1 \pmod p$ if and only if p is represented by one class in $S(m,n,d)$.

From Theorem 3.1 we know that $S(m,n,d) = G(u,v,d,1)$ is a subgroup of $H(-4k^2d)$. If $d = x^2$ for some integer x, then $(m+nx)(m-nx) = m^2 - dn^2 = -4$. This yields $m = 0$ and so $d \in \{1, 4\}$. Now assume $d \neq 1, 4$. Then d is a nonsquare integer. Note that $u^2 - dv^2 = -(2/(m,n))^2$ and $-d(u^2 - dv^2) = d(2/(m,n))^2$. We then see that $u^2 - dv^2$ and $-d(u^2 - dv^2)$ are nonsquare integers. Hence, by Theorem 3.1 we have $|S(m,n,d)| = |G(u,v,d,1)| = \frac{1}{4}h(-4k^2d)$. This completes the proof.

Remark 6.1 Let $d > 1$ be a squarefree integer, and $\varepsilon_d = (m + n\sqrt{d})/2$ with negative norm. Then clearly $m^2 - dn^2 = -4$. So, if $p \equiv 1 \pmod 4$ is a prime such that $(\frac{d}{p}) = 1$, it then follows from Theorem 6.2 that ε_d is a quadratic residue (mod p) if and only if p can be represented by one of the quadratic forms in the set $S(m,n,d)$. This generalizes all the special results scattered in the literature.

For instance, let $p \equiv 1 \pmod 4$ be a prime, $d \in \{2, 5, 10, 13, 17, 26, 29, 37, 41, 53\}$ and $(\frac{d}{p}) = 1$. Using Theorem 6.2 and the theory of reduced forms one can deduce that ε_d is a quadratic residue (mod p) if and only if p is represented by one of the corresponding quadratic forms in Table 2.

Table 2

ε_d	Corresponding quadratic forms
$\varepsilon_2 = 1 + \sqrt{2}$	$x^2 + 32y^2$
$\varepsilon_5 = \frac{1}{2}(1 + \sqrt{5})$	$x^2 + 20y^2$
$\varepsilon_{10} = 3 + \sqrt{10}$	$x^2 + 160y^2,\ 13x^2 + 6xy + 13y^2$
$\varepsilon_{13} = \frac{1}{2}(3 + \sqrt{13})$	$x^2 + 52y^2$
$\varepsilon_{17} = 4 + \sqrt{17}$	$x^2 + 68y^2,\ 4x^2 + 17y^2$
$\varepsilon_{26} = 5 + \sqrt{26}$	$x^2 + 416y^2,\ 21x^2 + 10xy + 21y^2,$ $5x^2 \pm 4xy + 84y^2,\ 17x^2 \pm 6xy + 25y^2$
$\varepsilon_{29} = \frac{1}{2}(5 + \sqrt{29})$	$x^2 + 116y^2,\ 5x^2 \pm 4xy + 24y^2$
$\varepsilon_{37} = 6 + \sqrt{37}$	$x^2 + 148y^2$
$\varepsilon_{41} = 32 + 5\sqrt{41}$	$x^2 + 164y^2,\ 4x^2 + 41y^2,\ 8x^2 \pm 4xy + 21y^2$
$\varepsilon_{53} = \frac{1}{2}(7 + \sqrt{53})$	$x^2 + 212y^2,\ 13x^2 \pm 6xy + 17y^2$

7. Applications to Lucas series.

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

$$u_0(a,b) = 0,\ u_1(a,b) = 1,\ u_{n+1}(a,b) = bu_n(a,b) - au_{n-1}(a,b)\ (n \geq 1)$$

and

$$v_0(a,b) = 2,\ v_1(a,b) = b,\ v_{n+1}(a,b) = bv_n(a,b) - av_{n-1}(a,b)\ (n \geq 1).$$

Set $d = b^2 - 4a$. It is well known that

$$u_n(a,b) = \frac{1}{\sqrt{d}}\Big\{\Big(\frac{b+\sqrt{d}}{2}\Big)^n - \Big(\frac{b-\sqrt{d}}{2}\Big)^n\Big\} \quad (d \neq 0) \tag{7.1}$$

and

$$v_n(a,b) = \Big(\frac{b+\sqrt{d}}{2}\Big)^n + \Big(\frac{b-\sqrt{d}}{2}\Big)^n. \tag{7.2}$$

Let p be an odd prime such that $(\frac{a}{p}) = 1$ and $p \nmid d$. In [Le] D.H. Lehmer showed that $p \mid u_{(p-(\frac{d}{p}))/2}(a,b)$. Thus, if $(\frac{4a-b^2}{p}) = 1$, then $p \mid u_{(p-(\frac{-1}{p}))/2}(a,b)$. Since $u_{2n}(a,b) = u_n(a,b)v_n(a,b)$ we see that $p \mid u_{(p-(\frac{-1}{p}))/4}(a,b)$ or $p \mid v_{(p-(\frac{-1}{p}))/4}(a,b)$. Now, a natural problem is to characterize those odd primes p such that $p \mid u_{(p-(\frac{-1}{p}))/4}(a,b)$.

Let $a, b \in \mathbb{Z}$, $ad \neq 0$, $a = 2^t a_0 (2 \nmid a_0)$, and let a' be the product of all the distinct odd prime divisors of a (if $a_0 = \pm 1$ we set $a' = 1$). From Definition 2.1 we see that

$$f(b,1,d) = \begin{cases} \frac{8}{(8,b)} & \text{if } 2 \nmid t, \\ \frac{4}{(2,(a_0+1+t)/2)} & \text{if } 2 \mid t \text{ and } 2 \nmid b, \\ 1 & \text{if } 2 \mid t \text{ and } 4 \mid b, \\ \frac{2}{(2,(a_0-1+t)/2)} & \text{if } 2 \mid t \text{ and } 2 \parallel b \end{cases} \quad \text{and } F(b,1,d) = \frac{a'}{(a',b)} f(b,1,d). \tag{7.3}$$

Theorem 7.1. *Let p be an odd prime, $a,b\in\mathbb{Z}$, $d=b^2-4a$, $p\nmid ad$, $p=Ax^2+2Bxy+Cy^2 (A,B,C,x,y\in\mathbb{Z})$, $(A,2ap)=1$ and $B^2-AC=-k^2d$, where $k=F(b,1,d)$ is given by (7.3). Then*

(i) $$u_{\frac{p-(\frac{-1}{p})}{2}}(a,b)\equiv\begin{cases}0\pmod p & \text{if } \left(\frac{B-kbi}{A}\right)_4=\pm1,\\ \mp\frac{2ky}{Ax+By}\left(\frac{-1}{p}\right)(-a)^{[\frac{p+1}{4}]}\pmod p & \text{if } \left(\frac{B-kbi}{A}\right)_4=\pm i,\end{cases}$$

(ii) $$u_{\frac{p+(\frac{-1}{p})}{2}}(a,b)\equiv\begin{cases}\pm(-a)^{[\frac{p}{4}]}\pmod p & \text{if } \left(\frac{B-kbi}{A}\right)_4=\pm1,\\ \mp\frac{kby}{Ax+By}(-a)^{[\frac{p}{4}]}\pmod p & \text{if } \left(\frac{B-kbi}{A}\right)_4=\pm i,\end{cases}$$

(iii) $$v_{\frac{p-(\frac{-1}{p})}{2}}(a,b)\equiv\begin{cases}\pm2(-a)^{[\frac{p+1}{4}]}\pmod p & \text{if } \left(\frac{B-kbi}{A}\right)_4=\pm1,\\ 0\pmod p & \text{if } \left(\frac{B-kbi}{A}\right)_4=\pm i,\end{cases}$$

(iv) $$v_{\frac{p+(\frac{-1}{p})}{2}}(a,b)\equiv\begin{cases}\pm\left(\frac{-1}{p}\right)(-a)^{[\frac{p}{4}]}b\pmod p & \text{if } \left(\frac{B-kbi}{A}\right)_4=\pm1,\\ \pm\left(\frac{-1}{p}\right)(-a)^{[\frac{p}{4}]}\frac{Ax+By}{ky}\pmod p & \text{if } \left(\frac{B-kbi}{A}\right)_4=\pm i.\end{cases}$$

Proof. Let $u=b$, $v=1$ and $s=(Ax+By)/(ky)$. Then clearly $s^2\equiv-d\pmod p$ since $Ap=(Ax+By)^2+k^2dy^2$. From the proof of Theorem 4.1 we see that $(Ap,y)=1$. Thus applying Theorem 2.1 and (7.3) we get

$$\left(\frac{s+bi}{p}\right)_4=\left(\frac{Ax+By+kbyi}{p}\right)_4=\left(\frac{B-kbi}{A}\right)_4.$$

From this and (2.9) we know that

$$\left(\frac{B-kbi}{A}\right)_4^2=\left(\frac{s+bi}{p}\right)_4^2=\left(\frac{s^2+b^2}{p}\right)=\left(\frac{b^2-d}{p}\right)=\left(\frac{a}{p}\right).$$

Now combining the above with [S2, Theorem 2.1] and [S2, Corollary 2.1] gives the result.

We remark that Theorem 2.1 of [S2] can be deduced from Theorem 4.1. So one may give a proof of Theorem 7.1 using Theorem 4.1 instead of [S2, Theorem 2.1].

From (7.3) one can verify the following lemma.

Lemma 7.1. *Let $a,b\in\mathbb{Z}$, $a(b^2-4a)\neq0$, $2^t\parallel a$, and*

$$\delta(a,b)=\begin{cases}\frac{8}{(8,b)} & \text{if } 2\nmid t,\\ 4 & \text{if } 2\mid t \text{ and } 2\nmid b,\\ \frac{2}{(2,\frac{a+1}{2}\cdot\frac{b}{2}-1)} & \text{if } 2\nmid a \text{ and } 2\mid b,\\ \frac{2}{(2,\frac{b}{2})} & \text{if } 2\mid t,\ 2\mid a \text{ and } 2\mid b.\end{cases}$$

Then

$$F(b,1,b^2-4a)\mid\delta(a,b)a'/(a',b)\quad\text{and}\quad 8\mid\delta(a,b)^2(b^2-4a),$$

where a' is the product of all the distinct odd prime divisors of a (if $a=\pm2^t$ we set $a'=1$).

Now we are able to prove the following general result.

Theorem 7.2. *Let p be an odd prime, $a, b \in \mathbb{Z}$, $d = b^2 - 4a$, and $p \nmid abd$. If $\delta(a,b)$ and a' are given in Lemma 7.1 and $k = \delta(a,b)a'/(a',b)$, then $p \mid u_{(p-(\frac{-1}{p}))/4}(a,b)$ if and only if p is represented by one class in the set*

$$G(a,b) = \Big\{ [A,2B,C] \;\Big|\; [A,2B,C] \in H(-4k^2d),\ (A,2a) = 1,\ \Big(\frac{kb+Bi}{A}\Big)_4 = 1 \Big\}.$$

Moreover, $G(a,b)$ is a subgroup of $H(-4k^2d)$; if a and $a(4a-b^2)$ are nonsquare integers, then $|G(a,b)| = \frac{1}{4}h(-4k^2d)$.

Proof. Set $u = b$ and $v = 1$. Since $p \nmid abd$ we know that (see [R]) $u_{p-(\frac{d}{p})}(a,b) \equiv 0 \pmod p$, $\quad u_p(a,b) \equiv (\frac{d}{p}) \pmod p$ and so $u_{p+(\frac{d}{p})}(a,b) \not\equiv 0 \pmod p$. It is well known that $u_m(a,b) \mid u_{km}(a,b)$ (see [R]). We thus have

$$p \mid u_{(p-(\frac{-1}{p}))/4}(a,b) \implies p \mid u_{p-(\frac{-1}{p})}(a,b) \implies \Big(\frac{-1}{p}\Big) = \Big(\frac{d}{p}\Big) \implies \Big(\frac{-d}{p}\Big) = 1.$$

If p is represented by one class in the set $G(a,b)$, we also have $(\frac{-d}{p}) = 1$. So we may assume $(\frac{-d}{p}) = 1$. From (7.1) we see that

$$p \;\Big|\; u_{\frac{p-(\frac{-1}{p})}{4}}(a,b) \iff \Big(\frac{u+v\sqrt{d}}{u-v\sqrt{d}}\Big)^{\frac{p-(\frac{-1}{p})}{4}} = \Big(\frac{b+\sqrt{d}}{b-\sqrt{d}}\Big)^{\frac{p-(\frac{-1}{p})}{4}} \equiv 1 \pmod p.$$

Hence applying Lemma 7.1 and Theorem 4.1 we see that $p \mid u_{(p-(\frac{-1}{p}))/4}(a,b)$ if and only if p is represented by one class in $G'(u,v,d,K)$, where $K = k/F(u,v,d)$. Since $G(a,b) = G'(u,v,d,K)$, $u^2 - dv^2 = 4a$ and $-d(u^2 - dv^2) = 4a(4a - b^2)$, applying Theorem 3.1 we obtain the result.

Remark 7.1 If $m \in \mathbb{Z} - \{0\}$, $m \mid b$, $m^2 \mid a$ and p is a prime such that $p \nmid m$, it follows from (7.1) that $p \mid u_n(a,b)$ if and only if $p \mid u_n(\frac{a}{m^2}, \frac{b}{m})$. Sometimes, using this observation we may decrease the discriminant of required quadratic forms.

Putting $a = -1$ in Theorem 7.2 we obtain the following result, which was announced in [S2].

Corollary 7.1. *Let p be a prime of the form $4m+1$, $b \in \mathbb{Z} - \{0\}$, $u_0 = 0$, $u_1 = 1$ and $u_{n+1} = bu_n + u_{n-1}$ $(n \ge 1)$. Then $p \mid u_{\frac{p-1}{4}}$ if and only if p is represented by some primitive, integral form $Ax^2 + 2Bxy + Cy^2$ of discriminant $-4(3-(-1)^b)^2(b^2+4)$ with the condition that $2 \nmid A$ and $\big(\frac{(3-(-1)^b)b+Bi}{A}\big)_4 = 1$. Moreover, the classes containing these primitive quadratic forms form a subgroup of index 4 in $H(-4(3-(-1)^b)^2(b^2+4))$.*

8. Criteria for $\varepsilon_d^{(p-(\frac{-1}{p}))/4} \pmod p$.

Let $d > 1$ be a squarefree integer, and let $\varepsilon_d = (m+n\sqrt{d})/2$ be such that $N(\varepsilon_d) = 1$. Then $m^2 - dn^2 = 4$. In this section we determine $\varepsilon_d^{(p-(\frac{-1}{p}))/4} \pmod p$, where p is an odd prime.

One can easily prove

Lemma 8.1. *Let $m, n, d \in \mathbb{Z}$ with $dn \neq 0$ and $m^2 - dn^2 = 4$. Then*

(i) $$\frac{m + n\sqrt{d}}{2} = \frac{\frac{n}{(n,m-2)}\sqrt{d} + \frac{m-2}{(n,m-2)}}{\frac{n}{(n,m-2)}\sqrt{d} - \frac{m-2}{(n,m-2)}} = \frac{\frac{m+2}{(n,m+2)} + \frac{n}{(n,m+2)}\sqrt{d}}{\frac{m+2}{(n,m+2)} - \frac{n}{(n,m+2)}\sqrt{d}}.$$

(ii) $$\mathrm{ord}_2(m-2) \geq \mathrm{ord}_2 n \quad \textit{or} \quad \mathrm{ord}_2(m+2) \geq \mathrm{ord}_2 n.$$

If $m, n, d \in \mathbb{Z},\ dn \neq 0$ and $m^2 - dn^2 = 4$, by Lemma 8.1 and the fact that $\mathrm{ord}_2(m+2) = \mathrm{ord}_2(-m-2)$ we may choose the sign of m such that $\mathrm{ord}_2(m-2) \geq \mathrm{ord}_2 n$.

Suppose $\mathrm{ord}_2(m-2) \geq \mathrm{ord}_2 n$, $m - 2 = 2^\alpha m_0 (2 \nmid m_0)$ and $n = 2^\beta n_0 (2 \nmid n_0)$. Using Definition 2.1 we can deduce that

$$F\Big(\frac{m-2}{(n, m-2)}, \frac{n}{(n, m-2)}, d\Big) = \begin{cases} \frac{8}{(4, m_0 - 1 - \alpha)} & \text{if } \alpha = \beta, \\ 4 & \text{if } \alpha = \beta + 1 \equiv 1 \pmod 2, \\ \frac{2(2,d)}{(4, d + m_0 - 1 - \alpha)} & \text{if } \alpha = \beta + 1 \equiv 0 \pmod 2, \\ \frac{2}{\gcd(2, d, \alpha)} & \text{if } \alpha = \beta + 2, \\ \frac{2}{(2,d)} & \text{if } \alpha \geq \beta + 3. \end{cases}$$

From this and the fact that $\alpha - \beta = \mathrm{ord}_2 d + \beta - \mathrm{ord}_2(m+2)$ one can verify the following result by considering the following six cases: (1) $8 \mid n$, (2) $2^2 \parallel n$ (so $4 \mid m-2$ and $2 \mid d$), (3) $2 \parallel n$ and $2 \nmid d$ (so $4 \mid m$ and $4 \mid d-3$), (4) $2 \parallel n$ and $2 \mid d$ (so $4 \mid m-2$ and $8 \mid d$), (5) $2 \nmid n$ and $2 \nmid d$ (so $2 \nmid m$ and $8 \mid d-5$), (6) $2 \nmid n$ and $2 \mid d$ (so $2 \mid m$ and $4 \mid d$).

Lemma 8.2. *Let $m, n, d \in \mathbb{Z},\ dn \neq 0,\ m^2 - dn^2 = 4$, and $\mathrm{ord}_2(m-2) \geq \mathrm{ord}_2 n$. If $g(m, n, d)$ is given by Table 3, then*

$$F((m-2)/(n, m-2), n/(n, m-2), d) = g(m, n, d).$$

Table 3

d	$g(m,n,d)$	*Corresponding conditions*
$d \equiv 0 \pmod 4$	4	$2^2 \parallel d,\ 2 \nmid n$
	2	$2^2 \parallel n,\ 8 \mid m+2$
		$2^3 \parallel d,\ 2 \parallel n$
	1	*Otherwise*
$d \equiv 1 \pmod 4$	4	$8 \mid d-5,\ 2 \nmid n,\ 4 \mid m-1$
	2	$8 \mid d-5,\ 2 \nmid n,\ 4 \mid m+1$
		$8 \mid n$
$d \equiv 2 \pmod 4$	4	$2^2 \parallel n$
	2	$2^3 \parallel n$
	1	$16 \mid n$
$d \equiv 3 \pmod 4$	8	$2 \parallel n$
	2	$8 \mid n$

Theorem 8.1. *Let p be an odd prime, and let $m^2-dn^2=4$ with $m,n,d\in\mathbb{Z}$ and $p\nmid dn$. We choose the sign of m so that $\mathrm{ord}_2(m-2)\ge \mathrm{ord}_2 n$. Let $g(m,n,d)\in\{1,2,4,8\}$ be given by Table 3, and $k=Kg(m,n,d)$ with $K\in\mathbb{Z}$ and $p\nmid K$.*

(1) *Assume that $p=ax^2+2bxy+cy^2 (a,b,c,x,y\in\mathbb{Z})$, $b^2-ac=-k^2d$, $(a, 2Kp\frac{8-4m}{(n,m-2)^2})=1$ and $j\in\{0,1,2,3\}$. Then*

$$\Big(\frac{m\pm n\sqrt{d}}{2}\Big)^{\frac{p-(\frac{-1}{p})}{4}}\equiv\Big(\pm(\frac{-1}{p})\frac{ax+by}{kdy}\sqrt{d}\Big)^j\pmod p\Leftrightarrow\Big(\frac{\frac{bn}{(n,m-2)}-k\frac{m-2}{(n,m-2)}i}{a}\Big)_4=i^j.$$

(2) *Suppose that $(\frac{-d}{p})=1$ and $\delta=\pm1$. Then $\big(\frac{\delta m+n\sqrt{d}}{2}\big)^{(p-(\frac{-1}{p}))/4}\equiv 1\pmod p$ if and only if p is represented by some class in the set $L_1(m,n,d,K)$ or $L_0(m,n,d,K)$ according as $(\frac{2}{p})=\delta=-1$ or not, where $L_j(m,n,d,K)(j=0,1)$ are given by*

$$L_j(m,n,d,K)=\Big\{[a,2b,c]\;\Big|\;\gcd(a,2b,c)=1,\ (2b)^2-4ac=-4k^2d,$$
$$\Big(a,\frac{2K(8-4m)}{(n,m-2)^2}\Big)=1,\ \Big(\frac{\frac{bn}{(n,m-2)}-k\frac{m-2}{(n,m-2)}i}{a}\Big)_4=(-1)^j\Big\}.$$

Moreover, $L_0(m,n,d,K)$ is a subgroup of $H(-4k^2d)$; if $2-m$ and $2+m$ are nonsquare integers, then $|L_0(m,n,d,K)|=|L_1(m,n,d,K)|=\frac14 h(-4k^2d)$.

Proof. Let $u=(m-2)/(n,m-2)$ and $v=n/(n,m-2)$. Then clearly $(u,v)=1$, $v\ne0$ and $u^2-dv^2=(8-4m)/(n,m-2)^2\not\equiv0\pmod p$ since $p\nmid dn$. From Lemmas 8.1 and 8.2 we see that $F(u,v,d)=g(m,n,d)$ and

$$\Big(\frac{v\sqrt{d}+u}{v\sqrt{d}-u}\Big)^{\frac{p-(\frac{-1}{p})}{4}}=\Big(\frac{m+n\sqrt{d}}{2}\Big)^{\frac{p-(\frac{-1}{p})}{4}}.$$

In addition, as $m^2-dn^2=4$ we have

$$\Big(\frac{m+n\sqrt{d}}{2}\Big)^{\frac{p-(\frac{-1}{p})}{4}}\Big(\frac{m-n\sqrt{d}}{2}\Big)^{\frac{p-(\frac{-1}{p})}{4}}=1.$$

Thus applying Theorem 4.1 we obtain (1). By (1),

$$\Big(\frac{\delta m+n\sqrt{d}}{2}\Big)^{\frac{p-(\frac{-1}{p})}{4}}\equiv1\pmod p\iff\Big(\frac{\frac{bn}{(n,m-2)}-k\frac{m-2}{(n,m-2)}i}{a}\Big)_4=\Big(\frac{2}{p}\Big)^{\frac{1-\delta}{2}}.$$

Hence (2) follows from (1), Theorem 3.1 and the proof of Theorem 4.1.

Corollary 8.1. *Let $p\equiv1\pmod4$ be a prime, $m,n,d\in\mathbb{Z}$, $m^2-dn^2=4$, $p\nmid n$ and $(\frac{d}{p})=1$. We choose the sign of m so that $\mathrm{ord}_2(m-2)\ge\mathrm{ord}_2 n$. For $\delta=\pm1$,*

$(\delta m + n\sqrt{d})/2$ *is a quartic residue* $(\mathrm{mod}\ p)$ *if and only if* p *is represented by one class in the set* $L_1(m,n,d,1)$ *or* $L_0(m,n,d,1)$ *according as* $(\frac{2}{p}) = \delta = -1$ *or not.*

Proof. Taking $K = 1$ in Theorem 8.1 and then using Euler's criterion leads to the result.

Let $m, n, d \in \mathbb{Z},\ m^2 - dn^2 = 4,\ dn \neq 0$ and $\mathrm{ord}_2(m+2) \geq \mathrm{ord}_2 n$. From Definition 2.1 and Lemma 8.2 we see that

$$F\Big(\frac{m+2}{(n,m+2)}, \frac{n}{(n,m+2)}, d\Big) = F\Big(\frac{-m-2}{(n,-m-2)}, \frac{n}{(n,-m-2)}, d\Big) = g(-m,n,d).$$

Thus one can easily deduce

Lemma 8.3. *Let* $m, n, d \in \mathbb{Z},\ m^2 - dn^2 = 4,\ dn \neq 0$ *and* $\mathrm{ord}_2(m+2) \geq \mathrm{ord}_2 n$. *If*

$$g'(m,n,d) = \begin{cases} 2 & \text{if } 8 \mid d,\ 8 \mid m-2 \text{ and } 8 \mid n-4, \\ \delta(n,d) & \text{otherwise} \end{cases}$$

and $\delta(n,d)$ *is given by Table* 4, *then*

$$F((m+2)/(n,m+2), n/(n,m+2), d) \mid g'(m,n,d) \quad \text{and} \quad 8 \mid g'(m,n,d)^2 d.$$

Table 4

d	$\delta(n,d)$	*Corresponding conditions*
$d \equiv 0 \pmod 8$	2	$2^3 \parallel d,\ 2 \parallel n$
	1	*Otherwise*
$d \equiv 4 \pmod 8$	4	$2 \nmid n$
	2	$2 \mid n$
$d \equiv 1 \pmod 4$	4	
$d \equiv 2 \pmod 4$	4	$2^2 \parallel n$
	2	$8 \mid n$
$d \equiv 3 \pmod 4$	8	$2 \parallel n$
	4	$8 \mid n$

Theorem 8.2. *Let* p *be an odd prime,* $m, n, d \in \mathbb{Z},\ m^2 - dn^2 = 4,\ p \nmid dn$, *and* $\mathrm{ord}_2(m+2) \geq \mathrm{ord}_2 n$. *Let* $g'(m,n,d)$ *be given in Lemma* 8.3.

(1) *Assume that*

$$p = ax^2 + 2bxy + cy^2 (a,b,c,x,y \in \mathbb{Z}), \quad b^2 - ac = -g'(m,n,d)^2 d,$$
$$\Big(a, 2p\frac{8+4m}{(n,m+2)^2}\Big) = 1 \quad \text{and} \quad j \in \{0,1,2,3\}.$$

Then

$$\Big(\frac{m+n\sqrt{d}}{2}\Big)^{\frac{p-(\frac{-1}{p})}{4}} \equiv \Big(\Big(\frac{-1}{p}\Big)\frac{ax+by}{g'(m,n,d)dy}\sqrt{d}\Big)^j \pmod p$$
$$\iff \Big(\frac{\frac{m+2}{(n,m+2)}g'(m,n,d)+\frac{bn}{(n,m+2)}i}{a}\Big)_4 = i^j.$$

(2) *Suppose that* $(\frac{-d}{p})=1$. *Then* $\big(\frac{m+n\sqrt{d}}{2}\big)^{(p-(\frac{-1}{p}))/4}\equiv 1 \pmod p$ *if and only if* p *is represented by one class in the set*

$$M(m,n,d)=\Big\{[a,2b,c] \;\Big|\; \gcd(a,2b,c)=1,\ (2b)^2-4ac=-4g'(m,n,d)^2d,$$
$$\Big(a,\frac{2(8+4m)}{(n,m+2)^2}\Big)=1,\ \Big(\frac{\frac{m+2}{(n,m+2)}g'(m,n,d)+\frac{bn}{(n,m+2)}i}{a}\Big)_4=1\Big\}.$$

Moreover, $M(m,n,d)$ *is a subgroup of* $H(-4g'(m,n,d)^2d)$; *if* $2-m$ *and* $2+m$ *are nonsquare integers, then* $|M(m,n,d)|=\frac{1}{4}h(-4g'(m,n,d)^2d)$.

Proof. Let $u=(m+2)/(n,m+2)$, $v=n/(n,m+2)$ and $k=g'(m,n,d)$. Then clearly $(u,v)=1$, $v\neq 0$ and $u^2-dv^2=(8+4m)/(n,m+2)^2\not\equiv 0 \pmod p$. From Lemmas 8.1 and 8.3 we know that

$$\frac{u+v\sqrt{d}}{u-v\sqrt{d}}=\frac{m+n\sqrt{d}}{2},\ F(u,v,d)\mid k \quad\text{and}\quad 8\mid k^2d.$$

So the result follows from Theorems 4.1 and 3.1.

Lemma 8.4. *Suppose* $a,b,c,d,k,m,n\in\mathbb{Z}$, $dn\neq 0$, $m^2-dn^2=4$, $(2b)^2-4ac=-4k^2d$ *and* $(a,2b)=1$. *Then*

(i) $$\Big(a,2k\frac{8-4m}{(n,m-2)^2}\Big)=\Big(a,2k\frac{8+4m}{(n,m+2)^2}\Big)=1.$$

(ii) $$\Big(\frac{k\frac{m+2}{(n,m+2)}+\frac{bn}{(n,m+2)}i}{a}\Big)_4=\Big(\frac{\frac{bn}{(n,m-2)}-k\frac{m-2}{(n,m-2)}i}{a}\Big)_4.$$

Proof. Let $d=2^{\mathrm{ord}_2 d}d_0$, $m-2=2^{\mathrm{ord}_2(m-2)}m_0$, $m+2=2^{\mathrm{ord}_2(m+2)}m_1$ and $n=2^{\mathrm{ord}_2 n}n_0$. Since

$$\frac{8\pm 4m}{(n,m\pm 2)^2}=\frac{(m\pm 2)^2}{(n,m\pm 2)^2}-d\frac{n^2}{(n,m\pm 2)^2}\in\mathbb{Z},$$
$$\frac{4m-8}{(n,m-2)^2}=2^{\mathrm{ord}_2\frac{4m-8}{(n,m-2)^2}}\frac{m_0}{(m_0,n_0)^2}\quad\text{and}\quad \frac{4m+8}{(n,m+2)^2}=2^{\mathrm{ord}_2\frac{4m+8}{(n,m+2)^2}}\frac{m_1}{(m_1,n_0)^2},$$

we see that both $m_0/(m_0,n_0)^2$ and $m_1/(m_1,n_0)^2$ are integers. From the fact that $m^2-dn^2=4$ we find $m_0m_1=d_0n_0^2$. Thus,

$$m_1\frac{m_0}{(m_0,n_0)^2}=d_0\Big(\frac{n_0}{(m_0,n_0)}\Big)^2\quad\text{and}\quad m_0\frac{m_1}{(m_1,n_0)^2}=d_0\Big(\frac{n_0}{(m_1,n_0)}\Big)^2.$$

Observing that

$$\Big(\frac{m_0}{(m_0,n_0)^2},\frac{n_0}{(m_0,n_0)}\Big)=\Big(\frac{m_1}{(m_1,n_0)^2},\frac{n_0}{(m_1,n_0)}\Big)=1,$$

we get

$$\frac{m_0}{(m_0,n_0)^2}\mid d_0\quad\text{and}\quad\frac{m_1}{(m_1,n_0)^2}\mid d_0.$$

Notice that $(a,k^2d)=(a,ac-b^2)=(a,-b^2)=1$ and so $(a,d_0)=(a,k)=1$. Then we obtain

$$\Big(a,\frac{m_0}{(m_0,n_0)^2}\Big)=\Big(a,\frac{m_1}{(m_1,n_0)^2}\Big)=1\quad\text{and so}\quad\Big(a,2k\frac{8\pm4m}{(n,m\pm2)^2}\Big)=1.$$

This proves (i).

Now consider (ii). Observe that

$$\begin{aligned}\Big(\frac{bn}{(n,m\pm2)}\Big)^2+\Big(\frac{k(m\pm2)}{(n,m\pm2)}\Big)^2&=\frac{(ac-k^2d)n^2+k^2(m\pm2)^2}{(n,m\pm2)^2}\\&\equiv\frac{-k^2(m^2-4)+k^2(m\pm2)^2}{(n,m\pm2)^2}=\frac{(8\pm4m)k^2}{(n,m\pm2)^2}\pmod{|a|}.\end{aligned}$$

In view of (i) we find

$$\Big(a,\Big(\frac{bn}{(n,m\pm2)}\Big)^2+\Big(\frac{k(m\pm2)}{(n,m\pm2)}\Big)^2\Big)=1$$

and hence

$$\Big(\frac{\frac{bn}{(n,m-2)}-k\frac{m-2}{(n,m-2)}i}{a}\Big)_4\Big(\frac{k\frac{m+2}{(n,m+2)}+\frac{bn}{(n,m+2)}i}{a}\Big)_4\neq0.$$

To see the result, we note that

$$\begin{aligned}&\Big(\frac{\frac{bn}{(n,m-2)}-k\frac{m-2}{(n,m-2)}i}{a}\Big)_4\Big(\frac{k\frac{m+2}{(n,m+2)}+\frac{bn}{(n,m+2)}i}{a}\Big)_4^{-1}\\&=\Big(\frac{\frac{bn}{(n,m-2)}-k\frac{m-2}{(n,m-2)}i}{a}\Big)_4\Big(\frac{k\frac{m+2}{(n,m+2)}-\frac{bn}{(n,m+2)}i}{a}\Big)_4\\&=\Big(\frac{\frac{(bn-k(m-2)i)(k(m+2)-bni)}{(n,m-2)(n,m+2)}}{a}\Big)_4=\Big(\frac{\frac{4kbn}{(n,m-2)(n,m+2)}-\frac{k^2(m^2-4)+b^2n^2}{(n,m-2)(n,m+2)}i}{a}\Big)_4\\&=\Big(\frac{\frac{4kbn}{(n,m-2)(n,m+2)}-\frac{n^2}{(n,m-2)(n,m+2)}aci}{a}\Big)_4=\Big(\frac{\frac{4kbn}{(n,m-2)(n,m+2)}}{a}\Big)_4=1.\\&\quad\text{(observe that } m^2-4=dn^2 \text{ and } b^2-ac=-k^2d)\end{aligned}$$

This completes the proof.

Theorem 8.3. *Let p be an odd prime, $m,n,d\in\mathbb{Z}$, $m^2-dn^2=4$, $p\nmid dn$, and let $\delta(n,d)\in\{1,2,4,8\}$ be given by Table 4.*

(1) *Assume that $p=ax^2+2bxy+cy^2 (a,b,c,x,y\in\mathbb{Z})$, $(a,2bp)=1$, $b^2-ac=-\delta(n,d)^2d$ and $j\in\{0,1,2,3\}$. Then*

$$\Big(\frac{m+n\sqrt{d}}{2}\Big)^{\frac{p-(\frac{-1}{p})}{4}}\equiv\Big(\Big(\frac{-1}{p}\Big)\frac{ax+by}{\delta(n,d)dy}\sqrt{d}\Big)^j \pmod p$$
$$\iff \Big(\frac{\frac{bn}{(n,m-2)}-\delta(n,d)\frac{m-2}{(n,m-2)}i}{a}\Big)_4=i^j.$$

(2) *Assume that $(\frac{-d}{p})=1$. Then $(\frac{m+n\sqrt{d}}{2})^{(p-(\frac{-1}{p}))/4}\equiv 1 \pmod p$ if and only if p is represented by some class in the set $N_j(m,n,d)$, where $j\in\{0,1\}$ is given by $p\equiv(-1)^j \pmod 4$ and*

$$N_j(m,n,d)=\Big\{[a,2b,c]\ \Big|\ b^2-ac=-\delta(n,d)^2d,\ a\equiv(-1)^j \pmod 4,$$
$$(a,b)=1,\ \Big(\frac{\frac{bn}{(n,m-2)}-\delta(n,d)\frac{m-2}{(n,m-2)}i}{a}\Big)_4=1\Big\}.$$

Moreover, if $2-m$ and $2+m$ are nonsquare integers, then $N_0(m,n,d)$ is a subgroup of index 4 or 8 in $H(-4\delta(n,d)^2d)$.

Proof. Set $k=\delta(n,d)$. We first prove (1). Let us consider the following three cases:

CASE 1. $\mathrm{ord}_2(m-2)\ge\mathrm{ord}_2 n$ and $g(m,n,d)\mid\delta(n,d)$. In this case, applying Lemma 8.4(i) and Theorem 8.1 we obtain the result.

CASE 2. $\mathrm{ord}_2(m-2)\ge\mathrm{ord}_2 n$ and $g(m,n,d)\nmid\delta(n,d)$. Comparing Tables 8.1 and 8.2 we find $8\mid d$, $2^2\parallel n$ and $8\mid m+2$. So $\mathrm{ord}_2(m+2)\ge 3\ge\mathrm{ord}_2 n$ and $\delta(n,d)=g'(m,n,d)=1$. Now applying Lemma 8.4 and Theorem 8.2 yields the desired result.

CASE 3. $\mathrm{ord}_2(m-2)<\mathrm{ord}_2 n$. In this case we have $\mathrm{ord}_2(m+2)\ge\mathrm{ord}_2 n$ by Lemma 8.1. From Lemma 8.3 we have $\delta(n,d)=g'(m,n,d)$. So the result follows from Lemma 8.4 and Theorem 8.2.

Now consider (2). Let $N(m,n,d)=N_0(m,n,d)\cup N_1(m,n,d)$. If $p=ax^2+2bxy+cy^2(a,b,c,x,y\in\mathbb{Z})$ with $a\equiv 1 \pmod 2$ and $b^2-ac=-k^2d$, then $ap=(ax+by)^2+k^2dy^2$. Since $8\mid k^2d$ by Table 8.2, we see that $ax+by\equiv 1 \pmod 2$ and so $ap\equiv(ax+by)^2\equiv 1 \pmod 8$. Hence we have $a\equiv p \pmod 8$. Thus for $j\in\{0,1\}$, $p\equiv(-1)^j \pmod 4$ is represented by some class in $N(m,n,d)$ if and only if p is represented by some class in $N_j(m,n,d)$. By the proof of (1), either $\mathrm{ord}_2(m-2)\ge\mathrm{ord}_2 n$ and $g(m,n,d)\mid\delta(n,d)$, or $\mathrm{ord}_2(m+2)\ge\mathrm{ord}_2 n$ and $\delta(n,d)=g'(m,n,d)$.

If $\mathrm{ord}_2(m-2)\ge\mathrm{ord}_2 n$ and $k=Kg(m,n,d)$ for some integer K, it follows from Theorem 8.1 that $(\frac{m+n\sqrt{d}}{2})^{(p-(\frac{-1}{p}))/4}\equiv 1 \pmod p$ if and only if p is represented by one class in the set $L_0(m,n,d,K)$, where $L_0(m,n,d,K)$ is given in Theorem 8.1. Let $u=(m-2)/(n,m-2)$ and $v=n/(n,m-2)$. Then $(u,v)=1$ and $u^2-dv^2=(8-4m)/(n,m-2)^2$. From Lemma 8.2 we know that $F(u,v,d)=g(m,n,d)$. Thus

$k = KF(u, v, d)$. Suppose that $(a, 2b, c)$ is a primitive quadratic form such that $(2b)^2 - 4ac = -4k^2d$, $(a, 2K(8-4m)/(n, m-2)^2) = 1$ and $\left(\frac{bv-kui}{a}\right)_4 = 1$. By Lemma 3.1 there is a primitive quadratic form $(a', 2b', c')$ satisfying $(a', 2d) = 1$ and $(a, 2b, c) \sim (a', 2b', c')$. Since $(a, 2b, c) \sim (a', 2b', c')$ we have $(2b')^2 - 4a'c' = (2b)^2 - 4ac = -4k^2d$. Therefore $(a', 2d) = 1$ if and only if $(a', 2b') = 1$. From Lemma 8.4 we see that $(a', 2b') = 1$ implies that $(a', 2k(8 - 4m)/(n, m - 2)^2) = 1$. Thus using Corollary 2.1 we obtain $\left(\frac{b'v-kui}{a'}\right)_4 = \left(\frac{bv-kui}{a}\right)_4 = 1$. So we have $N(m, n, d) = L_0(m, n, d, K)$. Hence combining the above, Theorem 8.1 and Lemma 3.4 gives the result.

If $\mathrm{ord}_2(m + 2) \geq \mathrm{ord}_2 n$ and $\delta(n, d) = g'(m, n, d)$, it follows from Theorem 8.2 that $(\frac{m+n\sqrt{d}}{2})^{(p-(\frac{-1}{p}))/4} \equiv 1 \pmod{p}$ if and only if p is represented by one class in the set $M(m, n, d)$. Set $u' = (m + 2)/(n, m + 2)$ and $v' = n/(n, m + 2)$. Then $(u', v') = 1$ and $u'^2 - dv'^2 = (8 + 4m)/(n, m + 2)^2$. By Lemma 8.3 we have $F(u', v', d) \mid k$ and $8 \mid k^2d$. Now, using Lemma 8.4, Theorem 3.1 and the above method, one can similarly prove that

$$M(m, n, d) = \Big\{ [a, 2b, c] \;\Big|\; b^2 - ac = -k^2d, (a, 2b) = 1, \Big(\frac{k\frac{m+2}{(n,m+2)} + \frac{bn}{(n,m+2)}i}{a} \Big)_4 = 1 \Big\}.$$

In view of Lemma 8.4 we see that $M(m, n, d) = N(m, n, d)$. Hence the result follows from the above, Theorem 8.2 and Lemma 3.4.

By the above we see that (2) is true. Hence the proof is complete.

Now using Corollary 8.1, Theorems 8.2, 8.3 and doing some calculations we have

Theorem 8.4. *Let p be a prime of the form $4k+1$, $d \in \{3, 6, 7, 11, 14, 15, 19, 21, 22, 23, 30, 31, 33, 34, 35, 38, 39, 42, 43, 46, 47\}$, and let ε_d be the fundamental unit of the quadratic field $\mathbb{Q}(\sqrt{d})$. Then ε_d is a quartic residue* (mod p) *if and only if p is represented by one of the corresponding quadratic forms in Table* 5.

Table 5

ε_d	*Corresponding quadratic forms*
$\varepsilon_3 = 2 + \sqrt{3}$	$x^2 + 192y^2$
$\varepsilon_6 = 5 + 2\sqrt{6}$	$x^2 + 96y^2$
$\varepsilon_7 = 8 + 3\sqrt{7}$	$x^2 + 448y^2$
$\varepsilon_{11} = 10 + 3\sqrt{11}$	$x^2 + 704y^2,\ 9x^2 \pm 8xy + 80y^2$
$\varepsilon_{14} = 15 + 4\sqrt{14}$	$x^2 + 56y^2$
$\varepsilon_{15} = 4 + \sqrt{15}$	$x^2 + 960y^2,\ 20x^2 + 20xy + 53y^2$
$\varepsilon_{19} = 170 + 39\sqrt{19}$	$x^2 + 1216y^2,\ 17x^2 \pm 10xy + 73y^2$
$\varepsilon_{21} = \frac{1}{2}(5 + \sqrt{21})$	$x^2 + 336y^2,\ 21x^2 + 16y^2$
$\varepsilon_{22} = 197 + 42\sqrt{22}$	$x^2 + 352y^2$
$\varepsilon_{23} = 24 + 5\sqrt{23}$	$x^2 + 1472y^2,\ 41x^2 \pm 4xy + 36y^2$
$\varepsilon_{30} = 11 + 2\sqrt{30}$	$x^2 + 480y^2,\ 5x^2 + 96y^2$
$\varepsilon_{31} = 1520 + 273\sqrt{31}$	$x^2 + 1984y^2,\ 41x^2 \pm 10xy + 49y^2$
$\varepsilon_{33} = 23 + 4\sqrt{33}$	$x^2 + 528y^2,\ 16x^2 + 16xy + 37y^2$
$\varepsilon_{34} = 35 + 6\sqrt{34}$	$x^2 + 544y^2,\ 17x^2 + 32y^2$
$\varepsilon_{35} = 6 + \sqrt{35}$	$x^2 + 2240y^2,\ 13x^2 \pm 6xy + 173y^2,$ $5x^2 + 448y^2,\ 36x^2 \pm 20xy + 65y^2$
$\varepsilon_{38} = 37 + 6\sqrt{38}$	$x^2 + 608y^2,\ 9x^2 \pm 4xy + 68y^2$
$\varepsilon_{39} = 25 + 4\sqrt{39}$	$x^2 + 156y^2$
$\varepsilon_{42} = 13 + 2\sqrt{42}$	$x^2 + 672y^2,\ 21x^2 + 32y^2$
$\varepsilon_{43} = 3482 + 531\sqrt{43}$	$x^2 + 2752y^2,\ 41x^2 \pm 12xy + 68y^2$
$\varepsilon_{46} = 24335 + 3588\sqrt{46}$	$x^2 + 736y^2,\ 4x^2 + 4xy + 185y^2$
$\varepsilon_{47} = 48 + 7\sqrt{47}$	$x^2 + 3008y^2,\ 36x^2 \pm 28xy + 89y^2,$ $49x^2 \pm 36xy + 68y^2$

In the end we pose some conjectures.

Conjecture 8.1 If $m, n, d \in \mathbb{Z},\ m^2 - dn^2 = 4$ and if $2 - m$ and $2 + m$ are nonsquare integers, then $|N_0(m, n, d)| = \frac{1}{8}h(-4\delta(n, d)^2 d)$.

For discriminant D let $H_4(D) = \{[a, b, c]^4 \mid [a, b, c] \in H(D)\}$ and $h_4(D) = |H_4(D)|$.

Conjecture 8.2 Let p be a prime of the form $8k + 1$. Then $h_4(-8p) = h_4(-128p) = h(-8p)/4$.

Conjecture 8.3 Let p be a prime of the form $24k+1$. Then $h_4(-24p) = h_4(-384p) = h(-24p)/8$.

Conjecture 8.4 Let p and q be primes of the form $4k + 1$ such that $(\frac{p}{q}) = 1$. Then $h_4(-4pq) = h_4(-64pq) = h(-4pq)/8$.

Conjecture 8.5 Let p and q be distinct primes of the form $8k + 1$. Then

$$h_4(-8pq) = h_4(-128pq) = \begin{cases} \frac{1}{16}h(-8pq) & \text{if } (\frac{p}{q}) = 1, \\ \frac{1}{8}h(-8pq) & \text{if } (\frac{p}{q}) = -1. \end{cases}$$

Conjecture 8.6 Let $d > 2$ be a squarefree integer. If $h_4(-64d)$ is odd, then $h_4(-64d) = h_4(-4d)$.

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*, John Wiley & Sons, Inc., New York, Chichester, 1998.

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

[Bu] D.A. Buell, *Binary Quadratic Forms*, Springer, New York, 1989.

[CI] Y. Chuman and N. Ishii, *On the quartic residue of quadratic units of negative norm*, Math. Japonica **32** (1987), 389-420.

[C] H. Cohen, *A Course in Computational Algebraic Number Theory*, Graduate Texts in Mathematics 138, Springer-Verlag, Berlin, New York, 1993.

[Cox] D.A. Cox, *Primes of the Form x^2+ny^2: Fermat, Class Field Theory, and Complex Multiplication*, John Wiley & Sons, Inc., New York, Chichester, 1989.

[D] P.G.L. Dirichlet, *Lectures on Number Theory* (*Supplements by R. Dedekind*), Translatd by J. Stillwell, American Mathematical Society, Providence, RI, 1999, pp. 217-221.

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

[H1] F. Halter-Koch, *Konstruktion von Klassenkorpern und Potenzrestkriterien fur quadratische Einheiten*, Manuscripta Math. **54** (1986), 453-492.

[H2] F. Halter-Koch, *On the quartic character of certain quadratic units and the representation of primes by binary quadratic forms*, Rocky Mountain J. Math. **16** (1986), 95-102.

[HI] F. Halter-Koch and N. Ishii, *Ring class fields modulo 8 of $\mathbf{Q}(\sqrt{-m})$ and the quartic character of units of $\mathbf{Q}(\sqrt{m})$ for $m\equiv 1$ mod 8*, Osaka J. Math. **26** (1989), 625-646.

[IR] K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory*, Springer, New York, 1982.

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

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

[Lem] 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.

[R] P. Ribenboim, *The Book of Prime Number Records*, 2nd ed., Springer, Berlin, 1989, pp. 44-50.

[S1] Z.H. Sun, *Supplements to the theory of quartic residues*, Acta Arith. **97** (2001), 361-377.

[S2] —, *Values of Lucas sequences modulo primes*, Rocky Mountain J. Math. **33** (2003), no. 3, 1123-1145.

[S3] —, *Combinatorial sum* $\sum_{\substack{k=0\\ k\equiv r(\mathrm{mod}\ m)}}^{n}\binom{n}{k}$ *and its applications in number theory II*, J. Nanjing Univ. Math. Biquarterly **10** (1993), 105-118.

[S4] —, *Notes on quartic residue symbol and rational reciprocity laws*, J. Nanjing Univ. Math. Biquarterly **9** (1992), 92-101.

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