J. Number Theory 124(2007), 62-104.

CUBIC RESIDUES AND BINARY QUADRATIC FORMS

ZHI-HONG SUN

Department of Mathematics, Huaiyin Teachers College,
Huaian, Jiangsu 223001, PR China
Received 21 October 2005; revised 22 July 2006

Communicated by David Goss

ABSTRACT. Let $p>3$ be a prime, $u,v,d\in\mathbb{Z}$, $\gcd(u,v)=1$, $p\nmid u^2-dv^2$ and $(\frac{-3d}{p})=1$, where $(\frac{a}{p})$ is the Legendre symbol. In the paper we mainly determine the value of $\big(\frac{u-v\sqrt{d}}{u+v\sqrt{d}}\big)^{(p-(\frac{p}{3}))/3} \pmod p$ by expressing p in terms of appropriate binary quadratic forms. As applications, for $p\equiv 1 \pmod 3$ we obtain a general criterion for $m^{(p-1)/3} \pmod p$ and a criterion for ε_d to be a cubic residue of p, where ε_d is the fundamental unit of the quadratic field $\mathbb{Q}(\sqrt{d})$. We also give a general criterion for $p\mid U_{(p-(\frac{p}{3}))/3}$, where $\{U_n\}$ is the Lucas sequence defined by $U_0=0$, $U_1=1$ and $U_{n+1}=PU_n-QU_{n-1}$ $(n\ge 1)$. Furthermore, we establish a general result to illustrate the connections between cubic congruences and binary quadratic forms.

MSC: Primary 11A15, Secondary 11E16, 11A07, 11B39
Keywords: cubic residue, binary quadratic form, cubic Jacobi symbol, cubic congruence

1. Introduction.

Let $\mathbb{Z}$ be the set of integers, $\omega=(-1+\sqrt{-3})/2$ and $\mathbb{Z}[\omega]=\{a+b\omega \mid a,b\in\mathbb{Z}\}$. For $\pi=a+b\omega\in\mathbb{Z}[\omega]$ the norm of π is given by $N\pi=\pi\bar\pi=a^2-ab+b^2$, where $\bar\pi$ is the complex conjugate of π. We recall that π is primary if $\pi\equiv 2 \pmod 3$ (that is, $3\mid a-2$ and $3\mid b$).

If $\pi\in\mathbb{Z}[\omega]$, $N\pi>1$ and $\pi\equiv\pm 2 \pmod 3$, we may write $\pi=\pm\pi_1\cdots\pi_r$, where $\pi_1,\ldots,\pi_r$ are primary primes. For $\alpha\in\mathbb{Z}[\omega]$, we can define the cubic Jacobi symbol

$$\Big(\frac{\alpha}{\pi}\Big)_3=\Big(\frac{\alpha}{\pi_1}\Big)_3\cdots\Big(\frac{\alpha}{\pi_r}\Big)_3,$$

E-mail: hyzhsun@public.hy.js.cn
URL: http://www.hytc.edu.cn/xsjl/szh/

where $\left(\frac{\alpha}{\pi_t}\right)_3$ is the cubic residue character of α modulo π_t defined by

$$\left(\frac{\alpha}{\pi_t}\right)_3 = \begin{cases} 0 & \text{if } \pi_t \mid \alpha, \\ \omega^i & \text{if } \alpha^{(N\pi_t-1)/3} \equiv \omega^i \pmod{\pi_t}. \end{cases}$$

For our convenience we also define $\left(\frac{\alpha}{1}\right)_3 = \left(\frac{\alpha}{-1}\right)_3 = 1$.

According to [IR, pp. 112-115, 135, 313] and [S1] the cubic Jacobi symbol has the following properties:

(1.1) If $a, b \in \mathbb{Z}$ and $a + b\omega \equiv 2 \pmod 3$, then

$$\left(\frac{\omega}{a+b\omega}\right)_3 = \omega^{\frac{a+b+1}{3}} \quad \text{and} \quad \left(\frac{1-\omega}{a+b\omega}\right)_3 = \omega^{\frac{2(a+1)}{3}}.$$

(1.2) If $\pi, \lambda \in \mathbb{Z}[\omega]$ and $\pi, \lambda \equiv \pm 2 \pmod 3$, then

$$\left(\frac{\lambda}{\pi}\right)_3 = \left(\frac{\pi}{\lambda}\right)_3.$$

(1.3) If $\alpha, \pi \in \mathbb{Z}[\omega]$ with $\pi \equiv \pm 2 \pmod 3$ and $(\frac{\alpha}{\pi})_3 \neq 0$, then

$$\left(\frac{\alpha}{\pi}\right)_3^{-1} = \overline{\left(\frac{\alpha}{\pi}\right)_3} = \left(\frac{\bar{\alpha}}{\bar{\pi}}\right)_3.$$

(1.4) If $m, n \in \mathbb{Z},\ 3 \nmid m$ and m is coprime to n, then $\left(\frac{n}{m}\right)_3 = 1$.

(1.5) If $\pi, \alpha, \beta \in \mathbb{Z}[\omega]$ and $\pi \equiv \pm 2 \pmod 3$, then $\left(\frac{\alpha\beta}{\pi}\right)_3 = \left(\frac{\alpha}{\pi}\right)_3 \left(\frac{\beta}{\pi}\right)_3$.

(1.6) If $\pi_1, \pi_2, \alpha \in \mathbb{Z}[\omega]$ and $\pi_i \equiv \pm 2 \pmod 3$ $(i = 1, 2)$, then

$$\left(\frac{\alpha}{\pi_1\pi_2}\right)_3 = \left(\frac{\alpha}{\pi_1}\right)_3 \left(\frac{\alpha}{\pi_2}\right)_3.$$

The assertion (1.2) is now called general cubic reciprocity law, which was first proved by G. Eisenstein.

For a prime $q > 3$ let $F_q = \mathbb{Z}/q\mathbb{Z}$ be the ring of residue classes modulo q and

$$C(q) = \{\infty\} \cup \{x \mid x \in F_q,\ x^2 \neq -3\}.$$

For $x, y \in C(q)$, in [S1] the author introduced the operation

$$x * y = \frac{xy - 3}{x + y} \quad (x * \infty = \infty * x = x)$$

and proved that $C(q)$ is a cyclic group of order $q - (\frac{q}{3})$, where $(\frac{a}{p})$ is the Legendre symbol.

Combining [S1, Corollary 2.1] with [S1, Theorem 3.2 and Corollary 3.3] we have

Theorem 1.1 (Rational cubic reciprocity law) Let p and q be distinct primes greater than 3. Suppose $p \equiv 1 \pmod 3$ and hence $4p = L^2 + 27M^2$ for some $L, M \in \mathbb{Z}$. Then

$$\begin{aligned} &q \text{ is a cubic residue modulo } p \\ &\iff \frac{L}{3M} \text{ is a cube in } C(q) \\ &\iff q \mid M \text{ or } \frac{L}{3M} \equiv \frac{s^3 - 9s}{3s^2 - 3} \pmod q \text{ for some } s \in \mathbb{Z}. \end{aligned}$$

Let p be a prime of the form $3k+1$. Let m be a cubefree integer with $m \not\equiv 0, \pm 1 \pmod p$. A general question is to give a good criterion for m to be a cubic residue of p. A more general problem is to determine the value of $m^{\frac{p-1}{3}}$ modulo p. Suppose $4p = L^2 + 27M^2$ with $L, M \in \mathbb{Z}$ and $L \equiv 1 \pmod 3$. Clearly $m^{\frac{p-1}{3}} \equiv 1, \frac{-1-L/(3M)}{2}, \frac{-1+L/(3M)}{2} \pmod p$. In [L1] E. Lehmer showed that if $L \equiv M \pmod 4$, then $2^{(p-1)/3} \equiv (L+9M)/(L-9M) \equiv \frac{-1-L/(3M)}{2} \pmod p$. When q is a prime and q is a cubic nonresidue of p, K. S. Williams [Wi] found a method to determine the sign of M so that $q^{\frac{p-1}{3}} \equiv \frac{-1-L/(3M)}{2} \pmod p$.

Inspired by Williams' work, in 1998 the author published the paper [S1]. From [S1, Corollaries 2.1, 3.3 and 3.4] we have the following result.

Theorem 1.2. *Let p and q be distinct primes greater than 3. Suppose $p \equiv 1 \pmod 3$, $4p = L^2 + 27M^2$ $(L, M \in \mathbb{Z})$, $L \equiv 1 \pmod 3$ and $q \nmid M$. For any $k \in \mathbb{Z}$ with $\left(\frac{k+1+2\omega}{q}\right)_3 = \omega$ (in particular, for $q \equiv \pm 4 \pmod 9$ we may take $k = 1$, for $q \equiv \pm 2 \pmod 9$ we may take $k = -1$, for $q \equiv \pm 4 \pmod 7$ we may take $k = 9$, for $q \equiv \pm 2 \pmod 7$ we may take $k = -9$), we have*

$$\begin{aligned} &q^{\frac{p-1}{3}} \equiv \frac{-1 - L/(3M)}{2} \pmod p \\ &\iff \frac{L}{3M} \equiv \frac{k(s^3 - 9s) - 9(s^2 - 1)}{s^3 - 9s + 3k(s^2 - 1)} \pmod q \quad \text{for some} \quad s \in \mathbb{Z}. \end{aligned}$$

In [S1] the author established the following general result for $m^{(p-1)/3} \pmod p$, see [S1, Theorem 2.1].

Theorem 1.3. *Let $p \equiv 1 \pmod 3$ be a prime and $4p = L^2 + 27M^2$ with $L, M \in \mathbb{Z}$ and $L \equiv 1 \pmod 3$. Suppose $m \in \mathbb{Z}$ and $p \nmid m$. Assume $2^\alpha \parallel m$, $3^\beta \parallel m$ and m' is the product of all prime divisors of m not dividing $6M$. Then for $i = 0, 1, 2$,*

$$\begin{aligned} &m^{\frac{p-1}{3}} \equiv \Big(\frac{-1 - L/(3M)}{2}\Big)^i \pmod p \\ &\iff \Big(\frac{L + 3M(1+2\omega)}{m'}\Big)_3 = \begin{cases} \omega^{i+\beta M} & \text{if } 2 \mid M, \\ \omega^{i+\beta M-\alpha} & \text{if } L \equiv M \pmod 4. \end{cases} \end{aligned}$$

In this paper we determine the value of $m^{\frac{p-1}{3}}$ modulo p by expressing p in terms of appropriate binary quadratic forms (see Theorem 4.4). For example, we have

$$10^{\frac{p-1}{3}}\equiv\begin{cases}1\pmod p & \text{if } p=x^2+75y^2,\ 3x^2+25y^2,\\ \frac{7x-2y}{10y}\pmod p & \text{if } p=7x^2+6xy+12y^2\neq 7,\\ -\frac{19x+6y}{10y}\pmod p & \text{if } p=19x^2+2xy+4y^2\neq 19,\end{cases}$$

where x and y are integers.

Let $p>3$ be a prime and $u,v,d\in\mathbb{Z}$ with $(u,v)=1$, $p\nmid u^2-dv^2$ and $(\frac{-3d}{p})=1$, where (u,v) is the greatest common divisor of u and v. In Section 4 we determine the value of $\big(\frac{u-v\sqrt{d}}{u+v\sqrt{d}}\big)^{(p-(\frac{p}{3}))/3}\pmod p$ by expressing p in terms of appropriate binary quadratic forms. For example, if p is a prime such that $p\equiv 2\pmod 3$ and $(\frac{p}{17})=-1$, then

$$(4+\sqrt{17})^{\frac{p+1}{3}}\equiv\begin{cases}-1\pmod p & \text{if } p=11x^2+5xy+11y^2,\\ \frac{1}{2}-\frac{10x+y}{102y}\sqrt{17}\pmod p & \text{if } p=5x^2+xy+23y^2\neq 5.\end{cases}$$

As applications, we obtain general criteria for $\varepsilon_d^{(p-(\frac{p}{3}))/3}\pmod p$ and $U_{(p-(\frac{p}{3}))/3}(P,Q)\pmod p$, where ε_d is the fundamental unit of the quadratic field $\mathbb{Q}(\sqrt{d})$ ($\mathbb{Q}$ denotes the set of rational numbers) and $\{U_n(P,Q)\}$ is the Lucas sequence given by $U_0(P,Q)=0$, $U_1(P,Q)=1$ and $U_{n+1}(P,Q)=PU_n(P,Q)-QU_{n-1}(P,Q)(n\geq 1)$.

For $a,b,c\in\mathbb{Z}$ denote the binary quadratic form $ax^2+bxy+cy^2$ by (a,b,c). The discriminant of (a,b,c) is the number $D=b^2-4ac$. Denote the equivalence class containing the form (a,b,c) by $[a,b,c]$. If a positive integer n is represented by (a,b,c), then n can be represented by any form in $[a,b,c]$. Thus we say that n is represented by $[a,b,c]$. For any nonsquare integer $D\equiv 0,1\pmod 4$ let $H(D)$ be the form class group consisting of classes of primitive, integral binary quadratic forms of discriminant D, and let $h(D)=|H(D)|$ be the corresponding class number.

In [SW1, SW2], using class field theory Spearman and Williams proved the following general result for cubic congruences.

Theorem 1.4 Let $a_1,a_2,a_3\in\mathbb{Z}$ be such that $f(x)=x^3+a_1x^2+a_2x+a_3$ is irreducible in $\mathbb{Z}[x]$. Let D be the discriminant of $f(x)$, and let d be the discriminant of the cubic field $\mathbb{Q}(t)$, where t is a root of $f(x)=0$. Then there is a unique subgroup $J(a_1,a_2,a_3)$ of index 3 in $H(d)$ such that if $p>3$ is a prime with $(\frac{D}{p})=1$, then the congruence $f(x)\equiv 0\pmod p$ has three solutions if and only if p is represented by one of the classes in $J(a_1,a_2,a_3)$.

In Section 7 of this paper, using our elementary method we prove a general result similar to Theorem 1.4. In particular, we construct the corresponding subgroup J.

All the main results in the paper are based on an important calculation concerning cubic Jacobi symbols, see Theorem 3.1. Using Theorem 3.1 we also construct cubic characters on $H(-3k^2d)$, where $k=k(u,v,d)$ is given by Definition 3.1. We should mention that some results in the paper are similar to those results for quartic residues in [S3].

In addition to the above notation, we also use throughout this paper the following notation:

$\mathbb{N}$—the set of positive integers, $\mathbb{Z}_m$—the set of those rational numbers whose denominator is coprime to m, $|x|$—the absolute value of x, $p^\alpha \parallel n$ means $p^\alpha \mid n$ but $p^{\alpha+1} \nmid n$, $\mathrm{ord}_p a$—the nonnegative integer r such that $p^r \parallel a$, $\gcd(n_1,n_2,n_3)$—the greatest common divisor of n_1,n_2,n_3, $(a,b,c)\sim(a',b',c')$ means (a,b,c) is equivalent to (a',b',c'), Ker χ—the kernel of the mapping χ.

2. Basic lemmas.

Let $p\in\mathbb{N}$, $3\nmid p$, $k\in\mathbb{Z}_p$ and $k\equiv k_0 \pmod p$ for $k_0\in\{0,1,\ldots,p-1\}$. Following [S1] we define $\left(\frac{k+1+2\omega}{p}\right)_3=\left(\frac{k_0+1+2\omega}{p}\right)_3$ and

$$C_i(p)=\Big\{k \;\Big|\; \Big(\frac{k+1+2\omega}{p}\Big)_3=\omega^i,\ k\in\mathbb{Z}_p\Big\} \quad \text{for} \quad i=0,1,2. \tag{2.1}$$

Lemma 2.1. *If a and b are integers such that $3\nmid a$ and $3\mid b$, then*

$$\Big(\frac{3}{a+b\omega}\Big)_3=\omega^{\frac{ab}{3}}.$$

Proof. Clearly $3=-\omega^2(1-\omega)^2$ and $\left(\frac{-1}{a+b\omega}\right)_3=1$. If $a\equiv 2 \pmod 3$, then $a+b\omega$ is primary. So using (1.1) we see that

$$\Big(\frac{3}{a+b\omega}\Big)_3=\Big(\frac{\omega}{a+b\omega}\Big)_3^2\Big(\frac{1-\omega}{a+b\omega}\Big)_3^2=\omega^{2(a+1+\frac{b}{3})}=\omega^{\frac{2b}{3}}=\omega^{\frac{ab}{3}}.$$

If $a\equiv 1 \pmod 3$, then $-a-b\omega$ is primary. We also have

$$\Big(\frac{3}{a+b\omega}\Big)_3=\Big(\frac{3}{-a-b\omega}\Big)_3=\omega^{\frac{(-a)(-b)}{3}}=\omega^{\frac{ab}{3}}.$$

This proves the lemma.

Lemma 2.2. *Let $u,v,d\in\mathbb{Z}$, and let $p>3$ be a prime such that $p\nmid u^2-dv^2$ and $(\frac{-3d}{p})=1$. Suppose $s\in\mathbb{Z}_p$ and $s^2\equiv -3d \pmod p$. Then*

$$\Big(\frac{u-v\sqrt{d}}{u+v\sqrt{d}}\Big)^{\frac{p-(\frac{p}{3})}{3}}\equiv\begin{cases}1 \pmod p & \text{if } \left(\frac{sv+u(1+2\omega)}{p}\right)_3=1,\\ \frac{1}{2}\big(-1-(\frac{p}{3})\frac{s\sqrt{d}}{d}\big) \pmod p & \text{if } \left(\frac{sv+u(1+2\omega)}{p}\right)_3=\omega,\\ \frac{1}{2}\big(-1+(\frac{p}{3})\frac{s\sqrt{d}}{d}\big) \pmod p & \text{if } \left(\frac{sv+u(1+2\omega)}{p}\right)_3=\omega^2.\end{cases}$$

Proof. If $p \mid u$, then $\left(\frac{sv+u(1+2\omega)}{p}\right)_3 = \left(\frac{sv}{p}\right)_3 = 1$ and $\left(\frac{u-v\sqrt{d}}{u+v\sqrt{d}}\right)^{(p-(\frac{p}{3}))/3} \equiv (-1)^{(p-(\frac{p}{3}))/3} = 1 \pmod{p}$. Thus the result holds when $p \mid u$. Now suppose $p \nmid u$. From [S1, Theorem 2.2] we know that for $i = 0, 1, 2$,

$$\frac{sv}{u} \in C_i(p) \iff \left(\frac{\frac{v}{u}s - \sqrt{-3}}{\frac{v}{u}s + \sqrt{-3}}\right)^{\frac{p-(\frac{p}{3})}{3}} \equiv \left(\frac{-1-(\frac{p}{3})\sqrt{-3}}{2}\right)^i \pmod{p}.$$

Since $s \equiv \pm\sqrt{-3} \cdot \sqrt{d} \pmod{p}$, we see that

$$\frac{sv}{u} \in C_i(p) \iff \left(\frac{\frac{v}{u}\sqrt{d} - 1}{\frac{v}{u}\sqrt{d} + 1}\right)^{\frac{p-(\frac{p}{3})}{3}} \equiv \left(\frac{-1-(\frac{p}{3})\frac{s}{\sqrt{d}}}{2}\right)^i \pmod{p}.$$

This yields the result.

Lemma 2.3. *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 $a_1u + a_2v + \frac{b_1+b_2}{2}w = t$. Let*

$$a_3 = \frac{a_1a_2}{t^2},\ b_3 = b_2 + 2\frac{a_2}{t}\left(\frac{b_1-b_2}{2}v - c_2w\right) \quad \text{and} \quad c_3 = \frac{b_3^2 - d}{4a_3}.$$

Then

$$[a_1, b_1, c_1][a_2, b_2, c_2] = [a_3, b_3, c_3].$$

Moreover, if $U, V \in \mathbb{Z}$ and $(a_1a_2, 9U^2 + 3dV^2) = 1$, then

$$\left(\frac{b_1V + U(1+2\omega)}{a_1}\right)_3\left(\frac{b_2V + U(1+2\omega)}{a_2}\right)_3 = \left(\frac{b_3V + U(1+2\omega)}{a_3}\right)_3.$$

Proof. From [C, p.246] we know that $[a_1, b_1, c_1][a_2, b_2, c_2] = [a_3, b_3, c_3]$. By [S3, Lemma 3.2], we have

$$b_3 \equiv b_1 \pmod{2a_1/t} \quad \text{and} \quad b_3 \equiv b_2 \pmod{2a_2/t}.$$

Thus,

$$\begin{aligned}
\left(\frac{b_3V + U(1+2\omega)}{a_3}\right)_3 &= \left(\frac{b_3V + U(1+2\omega)}{a_1/t}\right)_3\left(\frac{b_3V + U(1+2\omega)}{a_2/t}\right)_3 \\
&= \left(\frac{b_1V + U(1+2\omega)}{a_1/t}\right)_3\left(\frac{b_2V + U(1+2\omega)}{a_2/t}\right)_3 \\
&= \left(\frac{b_1V + U(1+2\omega)}{a_1}\right)_3\left(\frac{b_1V + U(1+2\omega)}{t}\right)_3^{-1} \\
&\quad \cdot \left(\frac{b_2V + U(1+2\omega)}{a_2}\right)_3\left(\frac{b_2V + U(1+2\omega)}{t}\right)_3^{-1} \\
&= \left(\frac{b_1V + U(1+2\omega)}{a_1}\right)_3\left(\frac{b_2V + U(1+2\omega)}{a_2}\right)_3 \\
&\quad \cdot \left(\frac{b_1V - U(1+2\omega)}{t}\right)_3\left(\frac{b_2V - U(1+2\omega)}{t}\right)_3.
\end{aligned}$$

Since $(a_i, 3(b_i^2V^2+3U^2)) = (a_i, 3(3U^2+dV^2)) = 1$ $(i = 1, 2)$ and $t \mid (b_1+b_2)$ we see that

$$\begin{aligned}
&\Big(\frac{b_1V - U(1+2\omega)}{t}\Big)_3\Big(\frac{b_2V - U(1+2\omega)}{t}\Big)_3\\
&= \Big(\frac{(b_1V - U(1+2\omega))(b_2V - U(1+2\omega))}{t}\Big)_3\\
&= \Big(\frac{b_1b_2V^2 - (b_1+b_2)UV(1+2\omega) - 3U^2}{t}\Big)_3\\
&= \Big(\frac{b_1b_2V^2 - 3U^2}{t}\Big)_3 = 1.
\end{aligned}$$

Hence the result follows.

Lemma 2.4. *Let $a, b \in \mathbb{Z}$ with $ab \neq 0$. Suppose*

$$F(a) = \prod_{3\nmid \operatorname{ord}_p a} p \prod_{\substack{\operatorname{ord}_p a \equiv 1 \pmod 3\\ p=3 \text{ or } \operatorname{ord}_p a \geq 4}} p,$$

where p runs over all distinct prime divisors of a. If $F(a) \nmid b$, then $x^3 - 3ax - ab$ is irreducible in $\mathbb{Z}[x]$.

Proof. For $i = 1, 2$ let

$$m_i = \prod_{\substack{p\mid a\\ \operatorname{ord}_p a \equiv i \pmod 3}} p,$$

where p runs over all distinct prime divisors of a such that $3 \mid (\operatorname{ord}_p a - i)$. Then clearly $a = m_1m_2^2n^3$ for some integer n. If $x^3-3ax-ab$ is irreducible in $\mathbb{Z}[x]$, then $x^3 - 3ax - ab = 0$ for some $x \in \mathbb{Z}$. For such an integer x we have $a \mid x^3$ and so $n^3 \mid x^3$. Hence $n \mid x$. Set $y = x/n$. Then $y \in \mathbb{Z}$ and $y^3 - 3m_1m_2^2ny - bm_1m_2^2 = 0$. Clearly $m_1m_2 \mid y^3$ and so $m_1m_2 \mid y$. Set $z = y/(m_1m_2)$. Then $z \in \mathbb{Z}$ and $m_1^2m_2z^3 - 3m_1m_2nz - b = 0$. Thus $m_1m_2(m_1, 3n) \mid b$. That is $F(a) \mid b$, which contradicts the assumption. Hence the lemma is proved.

Lemma 2.5. *Suppose $u, v, d \in \mathbb{Z}$, $dv(u^2 - dv^2) \neq 0$ and $(u, v) = 1$. Let $u^2 - dv^2 = 2^\alpha 3^r W (2 \nmid W, 3 \nmid W)$ and let w be the product of all distinct prime divisors of W. If $a, b, c, k, x, y \in \mathbb{Z}$, $b^2-4ac = -3k^2d$, $(a(ax^2+bxy+cy^2), 6ky(u^2 - dv^2)) = 1$, $3 \mid \frac{ku}{(k,v)}$ and $\frac{w}{(u,w)} \mid k$, then*

$$\begin{aligned}
&\Big(\frac{(2ax+by)v + kuy + 2kuy\omega}{ax^2+bxy+cy^2}\Big)_3\\
&= \begin{cases}
\omega^{\delta(\operatorname{ord}_3 k - \operatorname{ord}_3 v - r - 1)}\Big(\frac{bv - ku(1+2\omega)}{a}\Big)_3\\
\qquad\qquad \text{if } 2 \mid kuvdy,\\
\omega^{\pm(\alpha+1)+\delta(\operatorname{ord}_3 k - \operatorname{ord}_3 v - r - 1)}\Big(\frac{bv - ku(1+2\omega)}{a}\Big)_3\\
\qquad\qquad \text{if } 2 \nmid kuvdy \text{ and } x \equiv \frac{kuvb \pm 1}{2} \pmod 2,
\end{cases}
\end{aligned}$$

where

$$\delta = \frac{ku}{3(k,v)} \cdot \frac{v}{(k,v)}(2ax+by)y.$$

Proof. Since $3 \nmid a(ax^2+bxy+cy^2)$ and $4a(ax^2+bxy+cy^2) = (2ax+by)^2 + 3k^2dy^2$ we see that $3 \nmid 2ax+by$. Observing that $3 \mid \frac{ku}{(k,v)}$ and $(\frac{v}{(k,v)}, \frac{k}{(k,v)}u) = 1$ we find $3 \nmid \frac{v}{(k,v)}$ and hence $3 \nmid \frac{v}{(v,ky)}$.

Let

$$A = (2ax+by)\frac{v}{(v,ky)} \quad \text{and} \quad B = \frac{kuy}{(v,ky)} = \frac{ku}{(k,v)} \cdot \frac{y}{(v/(k,v),y)}.$$

By the above, it is clear that

$$A \equiv \pm 1 \pmod 3 \quad \text{and} \quad B \equiv 0 \pmod 3.$$

Notice that

$$(ax^2+bxy+cy^2, (v,ky)) = ((ax^2+bxy+cy^2, ky), v) = 1.$$

So we have

$$\Big(\frac{(2ax+by)v + kuy + 2kuy\omega}{ax^2+bxy+cy^2}\Big)_3 = \Big(\frac{A+B+2B\omega}{ax^2+bxy+cy^2}\Big)_3.$$

Since

$$\begin{aligned} &4a(ax^2+bxy+cy^2)\frac{v^2}{(v,ky)^2} \\ &= \big((2ax+by)^2 + 3k^2dy^2\big)\frac{v^2}{(v,ky)^2} \\ &= (2ax+by)^2\frac{v^2}{(v,ky)^2} + \frac{3k^2u^2y^2}{(v,ky)^2} + 3(dv^2-u^2)\frac{k^2y^2}{(v,ky)^2} \\ &= A^2 + 3B^2 + 3(dv^2-u^2)\frac{k^2y^2}{(v,ky)^2} \end{aligned} \tag{2.2}$$

and

$$(u,v) = (a(ax^2+bxy+cy^2), 3ky(u^2-dv^2)) = 1$$

we see that

$$\begin{aligned} &(a(ax^2+bxy+cy^2)v^2/(v,ky)^2,\ A^2+3B^2) \\ &\quad = (a(ax^2+bxy+cy^2)v^2/(v,ky)^2, 3(u^2-dv^2)k^2y^2/(v,ky)^2) = 1. \end{aligned}$$

Thus,

$$\Big(\frac{A+B+2B\omega}{a}\Big)_3\Big(\frac{A+B+2B\omega}{ax^2+bxy+cy^2}\Big)_3\Big(\frac{A+B+2B\omega}{v^2/(v,ky)^2}\Big)_3 \neq 0.$$

Hence

$$\Big(\frac{(2ax+by)v+kuy+2kuy\omega}{ax^2+bxy+cy^2}\Big)_3=\Big(\frac{A+B+2B\omega}{ax^2+bxy+cy^2}\Big)_3$$
$$=\Big(\frac{A+B+2B\omega}{a(ax^2+bxy+cy^2)v^2/(v,ky)^2}\Big)_3\Big(\frac{A+B+2B\omega}{av^2/(v,ky)^2}\Big)_3^{-1}.$$

Note that $3\nmid\frac{v}{(v,ky)}$ and $(a,ky)=1$. We see that

$$\begin{aligned}\Big(\frac{A+B+2B\omega}{av^2/(v,ky)^2}\Big)_3^{-1}&=\Big(\frac{A-B-2B\omega}{av^2/(v,ky)^2}\Big)_3\\&=\Big(\frac{A-B-2B\omega}{a}\Big)_3\Big(\frac{A-B-2B\omega}{v/(v,ky)}\Big)_3^2\\&=\Big(\frac{\frac{bvy}{(v,ky)}-\frac{kuy}{(v,ky)}(1+2\omega)}{a}\Big)_3\Big(\frac{-B(1+2\omega)}{v/(v,ky)}\Big)_3^2\\&=\Big(\frac{bvy-kuy(1+2\omega)}{a}\Big)_3\Big(\frac{-3B^2}{v/(v,ky)}\Big)_3\\&=\Big(\frac{bv-ku(1+2\omega)}{a}\Big)_3\end{aligned}$$

and

$$\mathrm{ord}_3\frac{ky}{(v,ky)}=\mathrm{ord}_3(ky)-\mathrm{ord}_3(v,ky)=\mathrm{ord}_3k+\mathrm{ord}_3y-\mathrm{ord}_3v.$$

Set $s=\mathrm{ord}_3k+\mathrm{ord}_3y-\mathrm{ord}_3v$. We may assume

$$\frac{ky}{(v,ky)}=2^\beta 3^sM(2\nmid M,3\nmid M).$$

If $A\not\equiv B\pmod 2$, we have

$$\Big(\frac{A+B+2B\omega}{4}\Big)_3=\Big(\frac{A+B+2B\omega}{2}\Big)_3^2=\Big(\frac{A+B}{2}\Big)_3^2=1.$$

Since

$$4a(ax^2+bxy+cy^2)\frac{v^2}{(v,ky)^2}\equiv(2ax+by)^2+3k^2dy^2\equiv1\pmod 3,$$

using (1.2), (1.4), (1.5), (1.6) and (2.2) we see that

$$\begin{aligned}&\Big(\frac{A+B+2B\omega}{a(ax^2+bxy+cy^2)v^2/(v,ky)^2}\Big)_3\\&=\Big(\frac{A+B+2B\omega}{4a(ax^2+bxy+cy^2)v^2/(v,ky)^2}\Big)_3=\Big(\frac{4a(ax^2+bxy+cy^2)v^2/(v,ky)^2}{A+B+2B\omega}\Big)_3\\&=\Big(\frac{A^2+3B^2+3(dv^2-u^2)k^2y^2/(v,ky)^2}{A+B+2B\omega}\Big)_3=\Big(\frac{3(dv^2-u^2)k^2y^2/(v,ky)^2}{A+B+2B\omega}\Big)_3\\&=\Big(\frac{2^{\alpha+2\beta}3^{r+2s+1}WM^2}{A+B+2B\omega}\Big)_3=\Big(\frac{2}{A+B+2B\omega}\Big)_3^{\alpha+2\beta}\Big(\frac{3^{r+2s+1}WM^2}{A+B+2B\omega}\Big)_3\\&=\Big(\frac{A+B+2B\omega}{2}\Big)_3^{\alpha+2\beta}\Big(\frac{3^{r+2s+1}WM^2}{A+B+2B\omega}\Big)_3=\Big(\frac{3^{r+2s+1}WM^2}{A+B+2B\omega}\Big)_3.\end{aligned}$$

If $A \equiv B \pmod 2$, then $4 \mid (A^2+3B^2)$ and $2 \nmid \frac{v}{(v,ky)}$. Applying (1.2) and (2.2) we see that

$$\begin{aligned}
&\Big(\frac{A+B+2B\omega}{a(ax^2+bxy+cy^2)v^2/(v,ky)^2}\Big)_3 \\
&= \Big(\frac{a(ax^2+bxy+cy^2)v^2/(v,ky)^2}{A+B+2B\omega}\Big)_3 = \Big(\frac{a(ax^2+bxy+cy^2)v^2/(v,ky)^2}{(A+B)/2+B\omega}\Big)_3 \\
&= \Big(\frac{\frac{1}{4}(A^2+3B^2)+\frac{3}{4}(dv^2-u^2)k^2y^2/(v,ky)^2}{(A+B)/2+B\omega}\Big)_3 = \Big(\frac{\frac{3}{4}(dv^2-u^2)k^2y^2/(v,ky)^2}{(A+B)/2+B\omega}\Big)_3 \\
&= \Big(\frac{2^{\alpha+2\beta-2}3^{r+2s+1}WM^2}{(A+B)/2+B\omega}\Big)_3 = \Big(\frac{2}{(A+B)/2+B\omega}\Big)_3^{\alpha+2\beta-2}\Big(\frac{3^{r+2s+1}WM^2}{A+B+2B\omega}\Big)_3.
\end{aligned}$$

By (1.1) and (1.2) we have

$$\begin{aligned}
\Big(\frac{2}{(A+B)/2+B\omega}\Big)_3 &= \Big(\frac{(A+B)/2+B\omega}{2}\Big)_3 \\
&= \begin{cases} \big(\frac{(A+B)/2}{2}\big)_3 = 1 & \text{if } 2 \mid B \text{ and } A+B \equiv 2 \pmod 4, \\ \big(\frac{1-\omega}{2}\big)_3 = \omega^2 & \text{if } AB \equiv 1 \pmod 4, \\ \big(\frac{\omega}{2}\big)_3 = \omega & \text{if } AB \equiv 3 \pmod 4. \end{cases}
\end{aligned}$$

If $2 \mid B$ and $A+B \equiv 0 \pmod 4$, as $\big(\frac{A+B+2B\omega}{a(ax^2+bxy+cy^2)v^2/(v,ky)^2}\big)_3 \neq 0$ we must have $\big(\frac{2^{\alpha+2\beta-2}}{(A+B)/2+B\omega}\big)_3 \neq 0$. But $\big(\frac{2}{(A+B)/2+B\omega}\big)_3 = 0$. Hence $\alpha+2\beta-2=0$. Thus, putting the above together we obtain

$$\begin{aligned}
&\Big(\frac{(2ax+by)v+kuy+2kuy\omega}{ax^2+bxy+cy^2}\Big)_3\Big(\frac{bv-ku(1+2\omega)}{a}\Big)_3^{-1} \\
&= \Big(\frac{A+B+2B\omega}{a(ax^2+bxy+cy^2)v^2/(v,ky)^2}\Big)_3 \\
&= \begin{cases} \big(\frac{3^{r+2s+1}WM^2}{A+B+2B\omega}\big)_3 & \text{if } AB \equiv 0 \pmod 2, \\ \omega^{2(\alpha+2\beta-2)}\big(\frac{3^{r+2s+1}WM^2}{A+B+2B\omega}\big)_3 & \text{if } AB \equiv 1 \pmod 4, \\ \omega^{\alpha+2\beta-2}\big(\frac{3^{r+2s+1}WM^2}{A+B+2B\omega}\big)_3 & \text{if } AB \equiv 3 \pmod 4. \end{cases}
\end{aligned}$$

Suppose that p is a prime divisor of W. Then clearly $p \mid w$. 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 $u^2 = dv^2 + 2^\alpha 3^r W$. But $(u,v)=1$, so $p \nmid v$. Hence $p \mid \frac{ku}{(k,v)}$ and therefore $p \mid B$. So we have

$$\begin{aligned}
\Big(\frac{W}{A+B+2B\omega}\Big)_3 &= \Big(\frac{A+B+2B\omega}{W}\Big)_3 = \prod_{p\mid W}\Big(\frac{A+B+2B\omega}{p}\Big)_3 \\
&= \prod_{p\mid W}\Big(\frac{A}{p}\Big)_3 = 1,
\end{aligned}$$

where in the products p runs over all prime divisors of W. As $M \mid B$ we have

$$\Big(\frac{M}{A+B+2B\omega}\Big)_3 = \Big(\frac{A+B+2B\omega}{M}\Big)_3 = \Big(\frac{A}{M}\Big)_3 = 1.$$

By Lemma 2.1 we also have

$$\Big(\frac{3}{A+B+2B\omega}\Big)_3 = \omega^{\frac{2B(A+B)}{3}} = \omega^{-\frac{AB}{3}}.$$

Thus

$$\begin{aligned}\Big(\frac{3^{r+2s+1}WM^2}{A+B+2B\omega}\Big)_3 &= \Big(\frac{3}{A+B+2B\omega}\Big)_3^{r+2s+1}\Big(\frac{W}{A+B+2B\omega}\Big)_3\Big(\frac{M}{A+B+2B\omega}\Big)_3^2\\ &= \omega^{-\frac{AB(r+2s+1)}{3}} = \omega^{\frac{AB}{3}(s-r-1)}.\end{aligned}$$

Note that $2 \nmid B$ implies $2 \nmid \frac{ky}{(v,ky)}$ and so $\beta = 0$. Combining the above we get

$$\begin{aligned}&\Big(\frac{(2ax+by)v+kuy+2kuy\omega}{ax^2+bxy+cy^2}\Big)_3\\ &= \begin{cases} \omega^{\frac{AB}{3}(s-r-1)}\big(\frac{bv-ku(1+2\omega)}{a}\big)_3 & \text{if } AB \equiv 0 \pmod 2,\\ \omega^{2(\alpha-2)+\frac{AB}{3}(s-r-1)}\big(\frac{bv-ku(1+2\omega)}{a}\big)_3 & \text{if } AB \equiv 1 \pmod 4,\\ \omega^{\alpha-2+\frac{AB}{3}(s-r-1)}\big(\frac{bv-ku(1+2\omega)}{a}\big)_3 & \text{if } AB \equiv 3 \pmod 4.\end{cases}\end{aligned}$$

Clearly

$$\begin{aligned}\frac{AB}{3} &= (2ax+by)\frac{v}{(v,ky)}\cdot\frac{kuy}{3(v,ky)} = \frac{ku}{3(k,v)}\cdot\frac{v}{(k,v)}\cdot\frac{(2ax+by)y}{(v/(k,v),y)^2}\\ &= \frac{\delta}{(v/(k,v),y)^2}.\end{aligned}$$

Since $3 \nmid \frac{v}{(k,v)}$ we see that $3 \nmid (\frac{v}{(k,v)}, y)$ and hence $(\frac{v}{(k,v)}, y)^2 \equiv 1 \pmod 3$. Thus

$$\frac{AB}{3} \equiv \delta \pmod 3.$$

If $2 \mid AB$, then clearly $2 \mid \delta$. Conversely, if $2 \mid \delta$, then $2 \mid AB$ when $2 \nmid (\frac{v}{(k,v)}, y)$. Since $2 \mid (\frac{v}{(k,v)}, y)$ implies $2 \mid y$ and so $2 \mid A$, we see that

$$2 \mid AB \iff 2 \mid \delta \quad \text{and hence} \quad 2 \nmid AB \iff 2 \nmid \delta.$$

When $2 \nmid \delta$, we must have $2 \nmid (\frac{v}{(k,v)}, y)$ and hence

$$\frac{AB}{3} = \frac{\delta}{(v/(k,v),y)^2} \equiv \delta \pmod 4.$$

From the above we obtain

$$\Big(\frac{(2ax+by)v+kuy+2kuy\omega}{ax^2+bxy+cy^2}\Big)_3$$
$$=\begin{cases}\omega^{\delta(s-r-1)}\big(\frac{bv-ku(1+2\omega)}{a}\big)_3 & \text{if } \delta\equiv 0 \pmod 2,\\ \omega^{2(\alpha-2)+\delta(s-r-1)}\big(\frac{bv-ku(1+2\omega)}{a}\big)_3 & \text{if } \delta\equiv 3 \pmod 4,\\ \omega^{\alpha-2+\delta(s-r-1)}\big(\frac{bv-ku(1+2\omega)}{a}\big)_3 & \text{if } \delta\equiv 1 \pmod 4.\end{cases}$$

If $3 \mid y$, since $3\nmid \frac{v}{(k,v)}$ we see that

$$\frac{B}{3}=\frac{ku}{3(k,v)}\cdot\frac{y}{(v/(k,v),y)}\equiv 0 \pmod 3 \quad \text{and} \quad \delta\equiv\frac{AB}{3}\equiv 0 \pmod 3.$$

Thus

$$\omega^{\delta s}=\omega^{\delta(\mathrm{ord}_3 y+\mathrm{ord}_3 k-\mathrm{ord}_3 v)}=\omega^{\delta(\mathrm{ord}_3 k-\mathrm{ord}_3 v)}.$$

Hence

$$\Big(\frac{(2ax+by)v+kuy+2kuy\omega}{ax^2+bxy+cy^2}\Big)_3$$
$$=\begin{cases}\omega^{\delta(\mathrm{ord}_3 k-\mathrm{ord}_3 v-r-1)}\big(\frac{bv-ku(1+2\omega)}{a}\big)_3 & \text{if } \delta\equiv 0 \pmod 2,\\ \omega^{\pm(\alpha+1)+\delta(\mathrm{ord}_3 k-\mathrm{ord}_3 v-r-1)}\big(\frac{bv-ku(1+2\omega)}{a}\big)_3 & \text{if } \delta\equiv \pm 1 \pmod 4.\end{cases}$$

To see the result, as $b^2-4ac=-3k^2d$ and $2\nmid a$ we note that

$$\delta\equiv\frac{ku}{3(k,v)}\cdot\frac{v}{(k,v)}\cdot by^2\equiv\frac{ku}{3(k,v)}\cdot\frac{v}{(k,v)}\cdot kdy\equiv kuvdy \pmod 2$$

and if $2\nmid kuvdy$, then

$$\delta\equiv\frac{kuv}{3}(2ax+by)y\equiv -kuv(2axy+b)\equiv 2x-kuvb \pmod 4.$$

3. Cubic characters on $H(-3k^2d)$.

For later convenience we first introduce the following notation.

Definition 3.1. *Suppose $u,v,d\in\mathbb{Z}$, $dv(u^2-dv^2)\neq 0$ and $(u,v)=1$. Let $u^2-dv^2=2^\alpha 3^r W(2\nmid W, 3\nmid W)$ and let w be the product of all distinct prime divisors of W. Define*

$$k_2(u,v,d)=\begin{cases}2 & \text{if } d\equiv 2,3 \pmod 4,\\ 2 & \text{if } d\equiv 1 \pmod 8,\ \alpha>0 \text{ and } \alpha\equiv 0,1 \pmod 3,\\ 1 & \text{otherwise,}\end{cases}$$

$$k_3(u,v,d)=\begin{cases}3^{\mathrm{ord}_3 v+1} & \text{if } 3\mid r \text{ and } 3\nmid u,\\ 9 & \text{if } 3\nmid r \text{ and } 3\nmid u,\\ 3 & \text{if } 3\nmid r-2 \text{ and } 3\parallel u,\\ 1 & \text{otherwise}\end{cases}$$

and $k(u,v,d)=k_2(u,v,d)k_3(u,v,d)w/(u,w)$.

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

Theorem 3.1. *Suppose* $u, v, d \in \mathbb{Z}$, $dv(u^2 - dv^2) \neq 0$ *and* $(u, v) = 1$. *If* $a, b, c, x, y \in \mathbb{Z}$, $k = k(u, v, d)$, $b^2 - 4ac = -3k^2d$ *and* $(a(ax^2 + bxy + cy^2), 6y(u^2 - dv^2)) = 1$, *then*

$$\Big(\frac{(2ax + by)v + kuy + 2kuy\omega}{ax^2 + bxy + cy^2}\Big)_3 = \Big(\frac{bv - ku - 2ku\omega}{a}\Big)_3.$$

Proof. Let

$$\delta = \frac{ku}{3(k, v)} \cdot \frac{v}{(k, v)}(2ax + by)y.$$

From Definition 3.1 we know that

$$3 \mid \frac{ku}{(k, v)}, \ \frac{w}{(u, w)} \mid k, \ \mathrm{ord}_3 k \geq \mathrm{ord}_3 v$$

and

$$\frac{ku}{3(k, v)}(\mathrm{ord}_3 k - \mathrm{ord}_3 v - r - 1) \equiv 0 \pmod 3.$$

Thus by Lemma 2.5 we have

$$\begin{aligned}
&\Big(\frac{(2ax + by)v + kuy + 2kuy\omega}{ax^2 + bxy + cy^2}\Big)_3 \\
&= \begin{cases} \big(\frac{bv - ku(1+2\omega)}{a}\big)_3 & \text{if } 2 \mid kuvdy, \\ \omega^{\pm(\alpha+1)}\big(\frac{bv - ku(1+2\omega)}{a}\big)_3 & \text{if } 2 \nmid kuvdy \text{ and } x \equiv \frac{kuvb \pm 1}{2} \pmod 2. \end{cases}
\end{aligned}$$

If $\alpha \equiv 0, 1 \pmod 3$, from Definition 3.1 we see that $2 \mid kuvd$. Thus we always have

$$\Big(\frac{(2ax + by)v + kuy + 2kuy\omega}{ax^2 + bxy + cy^2}\Big)_3 = \Big(\frac{bv - ku(1 + 2\omega)}{a}\Big)_3.$$

This completes the proof.

Corollary 3.1. *Suppose* $u, v, d \in \mathbb{Z}$, $dv(u^2 - dv^2) \neq 0$, $(u, v) = 1$ *and* $k = k(u, v, d)$. *If* $a, b, c, a', b', c' \in \mathbb{Z}$, $(a, b, c) \sim (a', b', c')$, $b^2 - 4ac = -3k^2d$ *and* $(aa', 6(u^2 - dv^2)) = 1$, *then*

$$\Big(\frac{b'v - ku(1 + 2\omega)}{a'}\Big)_3 = \Big(\frac{bv - ku(1 + 2\omega)}{a}\Big)_3.$$

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

$$\begin{aligned}
&a(\alpha X + \beta Y)^2 + b(\alpha X + \beta Y)(\gamma X + \delta Y) + c(\gamma X + \delta Y)^2 \\
&\quad = a'X^2 + b'XY + c'Y^2.
\end{aligned}$$

Hence

$$\begin{aligned} &a' = a\alpha^2 + b\alpha\gamma + c\gamma^2, \quad b' = 2a\alpha\beta + b(\alpha\delta + \beta\gamma) + 2c\gamma\delta, \\ &c' = a\beta^2 + b\beta\delta + c\delta^2. \end{aligned} \tag{3.1}$$

Set $a^* = a/(a,\gamma),\ c^* = (a,\gamma)c,\ x = \alpha$ and $y = \gamma/(a,\gamma)$. We see that

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

and

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

Hence

$$b'y = \frac{b'\gamma}{(a,\gamma)} \equiv -2\frac{a\alpha}{(a,\gamma)} - b\frac{\gamma}{(a,\gamma)} = -2a^*x - by \pmod{|a^*x^2 + bxy + c^*y^2|}.$$

Since $(aa', 6(u^2 - dv^2)) = 1$ we see that $(a^*(a^*x^2 + bxy + c^*y^2), 6(u^2 - dv^2)) = 1$. 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

$$(a^*(a^*x^2 + bxy + c^*y^2), 6y(u^2 - dv^2)) = 1.$$

Clearly we have $b^2 - 4a^*c^* = b^2 - 4ac = -3k^2d$. Thus, applying the above and Theorem 3.1 we get

$$\begin{aligned} &\Big(\frac{b'v - ku(1+2\omega)}{a'/(a,\gamma)}\Big)_3 \\ &= \Big(\frac{b'v - ku(1+2\omega)}{a^*x^2 + bxy + c^*y^2}\Big)_3 = \Big(\frac{-b'yv + kuy(1+2\omega)}{a^*x^2 + bxy + c^*y^2}\Big)_3 \\ &= \Big(\frac{(2a^*x + by)v + kuy(1+2\omega)}{a^*x^2 + bxy + c^*y^2}\Big)_3 = \Big(\frac{bv - ku(1+2\omega)}{a^*}\Big)_3 \\ &= \Big(\frac{bv - ku(1+2\omega)}{a/(a,\gamma)}\Big)_3. \end{aligned}$$

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

$$\begin{aligned} \Big(\frac{b'v - ku(1+2\omega)}{a'}\Big)_3 &= \Big(\frac{b'v - ku(1+2\omega)}{(a,\gamma)}\Big)_3\Big(\frac{b'v - ku(1+2\omega)}{a'/(a,\gamma)}\Big)_3 \\ &= \Big(\frac{bv - ku(1+2\omega)}{(a,\gamma)}\Big)_3\Big(\frac{bv - ku(1+2\omega)}{a/(a,\gamma)}\Big)_3 \\ &= \Big(\frac{bv - ku(1+2\omega)}{a}\Big)_3. \end{aligned}$$

This is the result.

Theorem 3.2. *Suppose $u, v, d \in \mathbb{Z}$, $dv(u^2 - dv^2) \neq 0$, $(u, v) = 1$ and $k = k(u, v, d)$. For $[a, b, c] \in H(-3k^2d)$ with $(a, 6(u^2 - dv^2)) = 1$ define $\chi([a, b, c]) = \big(\frac{bv-ku-2ku\omega}{a}\big)_3$. Then χ is a character on $H(-3k^2d)$. Moreover, if $F(u^2 - dv^2) \nmid 2u$, where $F(t)$ is given as in Lemma 2.4, then χ is a surjective homomorphism from $H(-3k^2d)$ to $\{1, \omega, \omega^2\}$.*

Proof. Let $[a, b, c] \in H(-3k^2d)$. By [S3, Lemma 3.1] we may assume $(a, 6(u^2 - dv^2)) = 1$ with no loss of generality. From Corollary 3.1 we see that χ is well defined. Since $b^2 - 4ac = -3k^2d$ we have

$$(bv-ku(1+2\omega))(bv+ku(1+2\omega)) = b^2v^2+3k^2u^2 \equiv 3k^2(u^2-dv^2) \pmod{|a|}$$

and so

$$\Big(\frac{bv - ku(1 + 2\omega)}{a}\Big)_3\Big(\frac{bv + ku(1 + 2\omega)}{a}\Big)_3 = \Big(\frac{3k^2(u^2 - dv^2)}{a}\Big)_3 = 1.$$

Thus $\chi([a, b, c]) \in \{1, \omega, \omega^2\}$. Applying Lemma 2.3 we find that χ is a character on $H(-3k^2d)$.

Since $F(u^2 - dv^2) \nmid 2u$, from Lemma 2.4 we see that $x^3 - 3(u^2 - dv^2)x - 2u(u^2 - dv^2)$ is irreducible over $\mathbb{Q}$. Thus, by [Se] there are infinitely many primes p such that $x^3-3(u^2-dv^2)x-2u(u^2-dv^2) \equiv 0 \pmod p$ is unsolvable. For such a prime p with $p \nmid 6duv(u^2 - dv^2)$, by [S1, Corollary 4.1] we have $-3((2u)^2 - 4(u^2 - dv^2)) \equiv (2u)^2x^2 \pmod p$ for some integer $x \in C_1(p)$. That is $-3dv^2 \equiv u^2x^2 \pmod p$ for some $x \in C_1(p)$. Let $b \in \mathbb{Z}$ be such that $bv \equiv -kux \pmod p$. Since $b \not\equiv b + p \pmod 2$ we may choose $b \in \mathbb{Z}$ such that $b \equiv kd \pmod 2$ and $bv \equiv -kux \pmod p$. Then $-bv/(ku) \in C_1(p)$ and $b^2 \equiv -3k^2d \pmod p$. Set $c = (b^2 + 3k^2d)/(4p)$. Then $c \in \mathbb{Z}$ and so $[p, b, c] \in H(-3k^2d)$. Clearly

$$\chi([p, b, c]) = \Big(\frac{bv - ku(1 + 2\omega)}{p}\Big)_3 = \Big(\frac{-\frac{bv}{ku} + 1 + 2\omega}{p}\Big)_3 = \omega.$$

Thus $\chi([p, b, c]^2) = \chi([p, b, c])^2 = \omega^2$ and $\chi([p, b, c]^3) = \chi([p, b, c])^3 = 1$. Hence χ is a surjective homomorphism from $H(-3k^2d)$ to $\{1, \omega, \omega^2\}$. This completes the proof.

Corollary 3.2. *Suppose $u, v, d \in \mathbb{Z}$, $dv(u^2 - dv^2) \neq 0$, $(u, v) = 1$ and $k = k(u, v, d)$. Let*

$$G(u, v, d) = \Big\{[a, b, c] \;\Big|\; [a, b, c] \in H(-3k^2d),\ (a, 6(u^2 - dv^2)) = 1,\ \Big(\frac{bv - ku(1 + 2\omega)}{a}\Big)_3 = 1\Big\}.$$

Then $G(u, v, d)$ is a subgroup of $H(-3k^2d)$. Moreover, if $F(u^2 - dv^2) \nmid 2u$, then $|G(u, v, d)| = h(-3k^2d)/3$ and so $3 \mid h(-3k^2d)$.

Proof. Let χ be the character given in Theorem 3.2. Then clearly $G(u, v, d) = \mathrm{Ker}\ \chi$. Thus $G(u, v, d)$ is a subgroup of $H(-3k^2d)$. If $F(u^2 -$

$dv^2) \nmid 2u$, then χ is a surjective homomorphism and so $H(-3k^2d)/\mathrm{Ker}\,\chi \cong \{1, \omega, \omega^2\}$. Hence $|G(u,v,d)| = h(-3k^2d)/3$. This finishes the proof.

Remark 3.1 Let χ be the character defined in Theorem 3.2. Let $A = \{K \mid K \in H(-3k^2d),\ K = K^{-1}\}$. For $K \in A$ we have $\chi(K) = \chi(K^{-1}) = \chi(K)^{-1}$ and so $\chi(K) = 1$. Thus A is a subgroup of $G(u,v,d)$. For $[a,b,c] \in H(-3k^2d)$ with $b = 0$, $a = b$ or $a = c$, we must have $[a,b,c] \in A$ and so $[a,b,c] \in G(u,v,d)$.

4. Criteria for $(\frac{u+v\sqrt{d}}{u-v\sqrt{d}})^{\frac{p-(\frac{p}{3})}{3}} \pmod p$.

Theorem 4.1. *Let $p > 3$ be a prime, $u, v, d \in \mathbb{Z}$, $(u,v) = 1$, $v \neq 0$, $p \nmid d(u^2 - dv^2)$, and let $k = k(u,v,d)$ be given by Definition 3.1. Let $a, b, c, x, y \in \mathbb{Z}$, $p = ax^2+bxy+cy^2$, $b^2-4ac = -3k^2d$ and $(a, 6(u^2-dv^2)) = 1$. If $p \nmid a$, then*

$$\left(\frac{u-v\sqrt{d}}{u+v\sqrt{d}}\right)^{\frac{p-(\frac{p}{3})}{3}} \equiv \Big(\frac{u^2-dv^2}{p}\Big)(u^2-dv^2)^{-\frac{p-(\frac{p}{3})}{6}}(u+v\sqrt{d})^{\frac{p-(\frac{p}{3})}{3}}$$

$$\equiv \begin{cases} 1 \pmod p & \text{if } \big(\frac{bv-ku(1+2\omega)}{a}\big)_3 = 1, \\ \frac{1}{2}\big(-1-(\frac{p}{3})\frac{2ax+by}{kdy}\sqrt{d}\big) \pmod p & \text{if } \big(\frac{bv-ku(1+2\omega)}{a}\big)_3 = \omega, \\ \frac{1}{2}\big(-1+(\frac{p}{3})\frac{2ax+by}{kdy}\sqrt{d}\big) \pmod p & \text{if } \big(\frac{bv-ku(1+2\omega)}{a}\big)_3 = \omega^2. \end{cases}$$

If $p \mid a$, then

$$\left(\frac{u-v\sqrt{d}}{u+v\sqrt{d}}\right)^{\frac{p-(\frac{p}{3})}{3}} \equiv \Big(\frac{u^2-dv^2}{p}\Big)(u^2-dv^2)^{-\frac{p-(\frac{p}{3})}{6}}(u+v\sqrt{d})^{\frac{p-(\frac{p}{3})}{3}}$$

$$\equiv \begin{cases} 1 \pmod p & \text{if } \big(\frac{bv-ku(1+2\omega)}{p}\big)_3 = 1, \\ \frac{1}{2}\big(-1+(\frac{p}{3})\frac{b\sqrt{d}}{kd}\big) \pmod p & \text{if } \big(\frac{bv-ku(1+2\omega)}{p}\big)_3 = \omega, \\ \frac{1}{2}\big(-1-(\frac{p}{3})\frac{b\sqrt{d}}{kd}\big) \pmod p & \text{if } \big(\frac{bv-ku(1+2\omega)}{p}\big)_3 = \omega^2. \end{cases}$$

Proof. As $p > 3$ and $p \nmid u^2 - dv^2$, we see that $p \nmid k$. If $p \mid a$, since $b^2 - 4ac = -3k^2d$ we have $b^2/k^2 \equiv -3d \pmod p$. Putting $s = -b/k$ in Lemma 2.2 we see that for $i = 0, 1, 2$,

$$\left(\frac{u-v\sqrt{d}}{u+v\sqrt{d}}\right)^{\frac{p-(\frac{p}{3})}{3}} \equiv \Big(\frac{-1+(\frac{p}{3})\frac{b\sqrt{d}}{kd}}{2}\Big)^i$$

$$\iff \Big(\frac{bv-ku(1+2\omega)}{p}\Big)_3 = \Big(\frac{-\frac{b}{k}v+u(1+2\omega)}{p}\Big)_3 = \omega^i.$$

Now assume $p \nmid a$. We first show that $p \nmid y$ and $(ax, y) = 1$. If $p \mid y$, then $p \mid x$ since $p \nmid a$. Hence $p = ax^2 + bxy + cy^2 \equiv 0 \pmod{p^2}$. But

this is impossible. So $p \nmid y$ and hence $(ax, y) = 1$ since $(ax, y) \mid p$. This together with $(a, 6(u^2 - dv^2)) = 1$ yields $(ap, 6y(u^2 - dv^2)) = 1$. Note that $4ap = (2ax+by)^2+3k^2dy^2$. We see that $(\frac{2ax+by}{ky})^2 \equiv -3d \pmod p$. Putting $s = \frac{2ax+by}{ky}$ in Lemma 2.2 and then applying Theorem 3.1 we get

$$\begin{aligned}
&\left(\frac{u - v\sqrt{d}}{u + v\sqrt{d}}\right)^{\frac{p-(\frac{p}{3})}{3}} \equiv \left(\frac{-1 - (\frac{p}{3})\frac{2ax+by}{kdy}\sqrt{d}}{2}\right)^i \pmod p \\
\iff &\Big(\frac{\frac{(2ax+by)v}{ky} + u(1+2\omega)}{p}\Big)_3 = \omega^i \\
\iff &\Big(\frac{(2ax+by)v + kuy(1+2\omega)}{p}\Big)_3 = \omega^i \\
\iff &\Big(\frac{bv - ku - 2ku\omega}{a}\Big)_3 = \omega^i,
\end{aligned}$$

where $i \in \{0, 1, 2\}$.

Now we claim that $(u + v\sqrt{d})^{p-(\frac{p}{3})} \equiv (u^2 - dv^2)^{(1-(\frac{p}{3}))/2} \pmod p$. If $p \equiv 1 \pmod 3$, then $(\frac{d}{p}) = (\frac{-3}{p}) = (\frac{p}{3}) = 1$. Since $p \nmid u^2 - dv^2$ we have $(u + v\sqrt{d})^{p-(\frac{p}{3})} \equiv 1 \pmod p$ by Fermat's little theorem. If $p \equiv 2 \pmod 3$, then $(\frac{d}{p}) = (\frac{-3}{p}) = (\frac{p}{3}) = -1$ and so $(\sqrt{d})^p = \sqrt{d} \cdot d^{\frac{p-1}{2}} \equiv -\sqrt{d} \pmod p$. Thus

$$\begin{aligned}
(u + v\sqrt{d})^{p-(\frac{p}{3})} &= (u + v\sqrt{d})(u + v\sqrt{d})^p \equiv (u + v\sqrt{d})(u^p + v^p(\sqrt{d})^p) \\
&\equiv (u + v\sqrt{d})(u - v\sqrt{d}) = u^2 - dv^2 \pmod p.
\end{aligned}$$

Hence the assertion is true and so

$$\begin{aligned}
\left(\frac{u - v\sqrt{d}}{u + v\sqrt{d}}\right)^{\frac{p-(\frac{p}{3})}{3}} &= \frac{(u^2 - dv^2)^{\frac{p-(\frac{p}{3})}{3}}}{(u + v\sqrt{d})^{\frac{2(p-(\frac{p}{3}))}{3}}} = \frac{(u^2 - dv^2)^{\frac{p-(\frac{p}{3})}{3}}(u + v\sqrt{d})^{\frac{p-(\frac{p}{3})}{3}}}{(u + v\sqrt{d})^{p-(\frac{p}{3})}} \\
&\equiv (u^2 - dv^2)^{\frac{p-(\frac{p}{3})}{3} - \frac{1-(\frac{p}{3})}{2}}(u + v\sqrt{d})^{\frac{p-(\frac{p}{3})}{3}} \\
&= (u^2 - dv^2)^{\frac{p-1}{2} - \frac{p-(\frac{p}{3})}{6}}(u + v\sqrt{d})^{\frac{p-(\frac{p}{3})}{3}} \\
&\equiv \Big(\frac{u^2 - dv^2}{p}\Big)(u^2 - dv^2)^{-\frac{p-(\frac{p}{3})}{6}}(u + v\sqrt{d})^{\frac{p-(\frac{p}{3})}{3}} \pmod p.
\end{aligned}$$

Now putting all the above together we prove the theorem.

Theorem 4.2. *Suppose that $p > 3$ is a prime, $u, v, d \in \mathbb{Z}$, $(u, v) = 1$, $v \neq 0$, $(\frac{-3d}{p}) = 1$, $p \nmid u^2 - dv^2$ and $k = k(u, v, d)$. Then $\left(\frac{u-v\sqrt{d}}{u+v\sqrt{d}}\right)^{(p-(\frac{p}{3}))/3} \equiv$*

$1 \pmod p$ *if and only if* p *is represented by some class in the set*

$$G(u,v,d)=\Big\{[a,b,c]\ \Big|\ [a,b,c]\in H(-3k^2d),\ (a,6(u^2-dv^2))=1,\\ \Big(\frac{bv-ku(1+2\omega)}{a}\Big)_3=1\Big\}.$$

Moreover, $G(u,v,d)$ *is a subgroup of* $H(-3k^2d)$. *If* $F(u^2-dv^2)\nmid 2u$, *then* $|G(u,v,d)|=h(-3k^2d)/3$.

Proof. Since $(\frac{-3d}{p})=1$ and $p\nmid k$, by the theory of binary quadratic forms and [S3, Lemma 3.1], p can be represented by some primitive quadratic form $ax^2+bxy+cy^2$ of discriminant $-3k^2d$ with $(a,6(u^2-dv^2))=1$, and there exists a primitive quadratic form (a',b',c') such that $(a',6p(u^2-dv^2))=1$ and $(a',b',c')\sim(a,b,c)$. As $(a',b',c')\sim(a,b,c)$, we see that $p=a'x'^2+b'x'y'+c'y'^2$ for some $x',y'\in\mathbb{Z}$ and $b'^2-4a'c'=b^2-4ac=-3k^2d$. Thus applying Theorem 4.1 and Corollary 3.1 we get

$$\Big(\frac{u-v\sqrt{d}}{u+v\sqrt{d}}\Big)^{\frac{p-(\frac{p}{3})}{3}}\equiv 1\pmod p\\ \iff \Big(\frac{b'v-ku(1+2\omega)}{a'}\Big)_3=1\iff\Big(\frac{bv-ku(1+2\omega)}{a}\Big)_3=1.$$

This together with Corollary 3.2 gives the result.

Corollary 4.1. *Suppose that* $p>3$ *is a prime,* $m\in\mathbb{Z}$, $p\nmid m(m+3)$, $s_p(m)\in\mathbb{Z}_p$ *and* $s_p(m)^2\equiv m\pmod p$. *Then the following statements are equivalent:*

(i) $s_p(m)\in C_0(p)$.

(ii) $\Big(\frac{3-\sqrt{-3m}}{3+\sqrt{-3m}}\Big)^{\frac{p-(\frac{p}{3})}{3}}\equiv 1\pmod p$.

(iii) p *is represented by some class* $[a,b,c]\in H(9k^2m)$ *with* $(a,6(m+3))=1$ *and* $\big(\frac{b-3k(1+2\omega)}{a}\big)_3=1$, *where* $k=k(3,1,-3m)$.

Proof. Putting $u=3$, $v=1$, $d=-3m$ and $s=3s_p(m)$ in Lemma 2.2 and Theorem 4.2 we obtain the result.

When $m=-1,-2,-5,-6,-7,-15$, the criteria for $s_p(m)\in C_0(p)$ have been given by the author in [S1, Theorem 5.2]. For example, $s_p(-1)\in C_0(p)$ if and only if p is represented by x^2+81y^2 or $2x^2+2xy+41y^2$.

Corollary 4.2. *Let* p *be a prime of the form* $3n+1$ *and* $4p=L^2+27M^2$ *with* $L,M\in\mathbb{Z}$. *Suppose* $d\in\mathbb{Z}$ *and* q *is a prime satisfying* $q>3$, $q\nmid d(d+3)$ *and* $q\mid(L^2-9dM^2)(-dL^2+81M^2)$. *Then* q *is a cubic residue*

of p if and only if q is represented by some class $[a,b,c] \in H(9k^2d)$ with $(a, 6(d+3)) = 1$ and $\left(\frac{b-3k(1+2\omega)}{a}\right)_3 = 1$, where $k = k(3,1,-3d)$.

Proof. From [S1, (5.4)] we know that q is a cubic residue of p if and only if $s_q(d) \in C_0(q)$, where $s_q(d) \in \mathbb{Z}$ satisfies $s_q(d)^2 \equiv d \pmod q$. Now applying Corollary 4.1 we obtain the result.

As an example, if $p \equiv 1 \pmod 3$ and $q > 5$ are primes with $4p = L^2 + 27M^2 (L, M \in \mathbb{Z})$ and $q \mid (L^2 + 135M^2)(5L^2 + 27M^2)$, then q is a cubic residue of p if and only if q is represented by $x^2 + 135y^2$ or $5x^2 + 27y^2$. See [S1, Theorem 5.3(ii)].

Now we can use Theorems 4.1 and 4.2 to deduce cubic residuacity.

Let p be a prime of the form $3k+1$ and $m, n \in \mathbb{Z}$ with $p \nmid mn$. Since mn^3 is a cubic residue of p if and only if m is a cubic residue of p, we need only to consider cubic residuacity for cubefree integers m with $m \not\equiv 1 \pmod 3$.

Lemma 4.1. *Let m be a cubefree integer with $m \neq 0, \pm 1$ and $m \not\equiv 1 \pmod 3$. Let m_0 be the product of all distinct primes q satisfying $q \mid m$ and $q > 3$. Then*

$$k\Big(\frac{1+m}{(2,1+m)}, \frac{1-m}{(2,1+m)}, 1\Big) = \frac{3+(-1)^m}{2} k_3 m_0,$$

where

$$k_3 = \begin{cases} 1 & \text{if } m \equiv 8 \pmod 9, \\ 3 & \text{if } m \equiv 2, 5 \pmod 9, \\ 9 & \text{if } m \equiv 0 \pmod 3. \end{cases} \tag{4.1}$$

Proof. Let $u = (1+m)/(1+m, 2)$, $v = (1-m)/(1+m, 2)$ and $d = 1$. It is easily seen that

$$(u, v) = 1, \ \frac{u - v\sqrt{d}}{u + v\sqrt{d}} = m, \ u^2 - dv^2 = \begin{cases} m & \text{if } 2 \nmid m, \\ 4m & \text{if } 2 \mid m. \end{cases} \tag{4.2}$$

Since m is cubefree, we have $\mathrm{ord}_2 m \in \{0, 1, 2\}$. Thus, by Definition 3.1 we have

$$k_2(u, v, d) = \frac{3+(-1)^m}{2} = \begin{cases} 1 & \text{if } 2 \nmid m, \\ 2 & \text{if } 2 \mid m. \end{cases}$$

As $\mathrm{ord}_3 m \in \{0, 1, 2\}$, from Definition 3.1 we see that $k_3(u, v, d) = k_3$. Now the result follows from the above and Definition 3.1.

Theorem 4.3. *Let $p \equiv 1 \pmod 3$ be a prime. Let m be a cubefree integer with $m \not\equiv 0, \pm 1 \pmod p$ and $m \not\equiv 1 \pmod 3$. Let m_0 be the product of all distinct primes q satisfying $q \mid m$ and $q > 3$. Let k_3 be given by* (4.1)

and $k=\frac{3+(-1)^m}{2}k_3m_0$. *Suppose* $p=ax^2+bxy+cy^2$ *with* $a,b,c,x,y\in\mathbb{Z}$, $b^2-4ac=-3k^2$ *and* $(a,6m)=1$. *If* $p\nmid a$, *then*

$$m^{\frac{p-1}{3}}\equiv\begin{cases}1\pmod p & \text{if } \left(\frac{(m-1)b+k(m+1)(1+2\omega)}{a}\right)_3=1,\\ -\frac{ax+(k+b)y/2}{ky}\pmod p & \text{if } \left(\frac{(m-1)b+k(m+1)(1+2\omega)}{a}\right)_3=\omega,\\ \frac{ax-(k-b)y/2}{ky}\pmod p & \text{if } \left(\frac{(m-1)b+k(m+1)(1+2\omega)}{a}\right)_3=\omega^2.\end{cases}$$

If $p\mid a$, *then*

$$m^{\frac{p-1}{3}}\equiv\begin{cases}1\pmod p & \text{if } \left(\frac{(m-1)b+k(m+1)(1+2\omega)}{p}\right)_3=1,\\ \frac{b-k}{2k}\pmod p & \text{if } \left(\frac{(m-1)b+k(m+1)(1+2\omega)}{p}\right)_3=\omega,\\ -\frac{b+k}{2k}\pmod p & \text{if } \left(\frac{(m-1)b+k(m+1)(1+2\omega)}{p}\right)_3=\omega^2.\end{cases}$$

Proof. Let $u=(1+m)/(1+m,2)$, $v=(1-m)/(1+m,2)$ and $d=1$. By (4.2), Lemma 4.1 and Theorem 4.1 we obtain the result.

From Theorem 4.3 and the theory of reduced forms we deduce the following results.

Corollary 4.3. *Let* p *be a prime of the form* $3n+1$. *Then*

$$2^{\frac{p-1}{3}}\equiv\begin{cases}1\pmod p & \text{if } p=x^2+27y^2,\\ \frac{7x-2y}{6y}\pmod p & \text{if } p=7x^2+2xy+4y^2\neq 7,\end{cases}$$

$$3^{\frac{p-1}{3}}\equiv\begin{cases}1\pmod p & \text{if } p=x^2+xy+61y^2,\\ -\frac{7x+6y}{9y}\pmod p & \text{if } p=7x^2+3xy+9y^2\neq 7,\end{cases}$$

$$5^{\frac{p-1}{3}}\equiv\begin{cases}1\pmod p & \text{if } p=x^2+xy+169y^2,\ 13x^2+xy+13y^2,\\ \frac{19x-6y}{15y}\pmod p & \text{if } p=19x^2+3xy+9y^2\neq 19,\\ \frac{7x-5y}{15y}\pmod p & \text{if } p=7x^2+5xy+25y^2\neq 7,\end{cases}$$

$$6^{\frac{p-1}{3}}\equiv\begin{cases}1\pmod p & \text{if } p=x^2+243y^2,\ 7x^2+6xy+36y^2,\\ -\frac{13x+11y}{18y}\pmod p & \text{if } p=13x^2+4xy+19y^2\neq 13,\\ -\frac{61x+10y}{18y}\pmod p & \text{if } p=61x^2+2xy+4y^2\neq 61,\\ \frac{31x-3y}{18y}\pmod p & \text{if } p=31x^2+12xy+9y^2\neq 31.\end{cases}$$

Corollary 4.4. *Let p be a prime of the form $3n+1$. Then*

$$7^{\frac{p-1}{3}} \equiv \begin{cases} 1 \pmod p & \text{if } p = x^2+xy+331y^2,\ 19x^2+11xy+19y^2, \\ \frac{37x-9y}{21y} \pmod p & \text{if } p = 37x^2+3xy+9y^2 \neq 37, \\ -\frac{13x+15y}{21y} \pmod p & \text{if } p = 13x^2+9xy+27y^2 \neq 13, \end{cases}$$

$$10^{\frac{p-1}{3}} \equiv \begin{cases} 1 \pmod p & \text{if } p = x^2+75y^2,\ 3x^2+25y^2, \\ \frac{7x-2y}{10y} \pmod p & \text{if } p = 7x^2+6xy+12y^2 \neq 7, \\ -\frac{19x+6y}{10y} \pmod p & \text{if } p = 19x^2+2xy+4y^2 \neq 19, \end{cases}$$

$$17^{\frac{p-1}{3}} \equiv \begin{cases} 1 \pmod p & \text{if } p = x^2+xy+217y^2,\ 3x^2+3xy+73y^2, \\ -\frac{7x+9y}{17y} \pmod p & \text{if } p = 7x^2+xy+31y^2 \neq 7, \\ -\frac{13x+14y}{17y} \pmod p & \text{if } p = 13x^2+11xy+19y^2 \neq 13. \end{cases}$$

Remark 4.1. *Let $p \equiv 1 \pmod 3$ be a prime and $4p = L^2+27M^2$ with $L, M \in \mathbb{Z}$ and $L \equiv 1 \pmod 3$. When $2 \nmid M$ we choose the sign of M so that $M \equiv L \pmod 4$. From Theorem 1.3 and [S1, Example 2.1] (or [Wi]) we deduce*

$$2^{\frac{p-1}{3}} \equiv \begin{cases} 1 \pmod p & \text{if } 2 \mid M, \\ \frac{1}{2}\big(-1-\frac{L}{3M}\big) \pmod p & \text{if } 2 \nmid M, \end{cases}$$

$$3^{\frac{p-1}{3}} \equiv \begin{cases} 1 \pmod p & \text{if } 3 \mid M, \\ \frac{1}{2}\big(-1\pm\frac{L}{3M}\big) \pmod p & \text{if } M \equiv \pm 1 \pmod 3, \end{cases}$$

$$5^{\frac{p-1}{3}} \equiv \begin{cases} 1 \pmod p & \text{if } 5 \mid LM, \\ \frac{1}{2}\big(-1\mp\frac{L}{3M}\big) \pmod p & \text{if } \frac{L}{3M} \equiv \pm 1, \pm 2 \pmod 5, \end{cases}$$

$$6^{\frac{p-1}{3}} \equiv \begin{cases} 1 \pmod p & \text{if } M \equiv 0, 1 \pmod 6, \\ \frac{1}{2}\big(-1-\frac{L}{3M}\big) \pmod p & \text{if } M \equiv 2, 3 \pmod 6, \\ \frac{1}{2}\big(-1+\frac{L}{3M}\big) \pmod p & \text{if } M \equiv 4, 5 \pmod 6. \end{cases}$$

For $p \neq 7$ we also have

$$7^{\frac{p-1}{3}} \equiv \begin{cases} 1 \pmod p & \text{if } 7 \mid LM, \\ \frac{1}{2}\big(-1\pm\frac{L}{3M}\big) \pmod p & \text{if } \frac{L}{3M} \equiv \pm 1, \pm 4 \pmod 7, \end{cases}$$

$$10^{\frac{p-1}{3}} \equiv \begin{cases} 1 \pmod p & \text{if } 2 \mid M \text{ and } 5 \mid LM, \\ & \quad \text{or if } 2 \nmid M \text{ and } \frac{L}{3M} \equiv -1, -2 \pmod 5, \\ \frac{1}{2}\big(-1-\frac{L}{3M}\big) \pmod p & \text{if } 2 \mid M \text{ and } \frac{L}{3M} \equiv 1, 2 \pmod 5, \\ & \quad \text{or if } 2 \nmid M \text{ and } 5 \mid LM, \\ \frac{1}{2}\big(-1+\frac{L}{3M}\big) \pmod p & \text{if } 2 \mid M \text{ and } \frac{L}{3M} \equiv -1, -2 \pmod 5, \\ & \quad \text{or if } 2 \nmid M \text{ and } \frac{L}{3M} \equiv 1, 2 \pmod 5, \end{cases}$$

$$17^{\frac{p-1}{3}} \equiv \begin{cases} 1 \pmod p & \text{if } 17 \mid LM \text{ or } \frac{L}{3M} \equiv \pm 1, \pm 3 \pmod{17}, \\ \frac{1}{2}\big(-1\mp\frac{L}{3M}\big) \pmod p & \text{if } \pm\frac{L}{3M} \equiv 2, 4, -5, -6, 7, -8 \pmod{17}. \end{cases}$$

Now let us compare these results with Corollaries 4.3 and 4.4. As $4(7x^2+2xy+4y^2)=(x+4y)^2+27x^2$ and $4(7x^2+3xy+9y^2)=(x+6y)^2+27x^2$, it is easily seen that the above results for $2^{\frac{p-1}{3}},\ 3^{\frac{p-1}{3}} \pmod p$ are equivalent to those given in Corollary 4.3. As for $10^{\frac{p-1}{3}}, 17^{\frac{p-1}{3}} \pmod p$, the results in Corollary 4.4 are better than the above results. For general results concerning $m^{\frac{p-1}{3}} \pmod p$, Theorem 4.3 seems better than Theorem 1.3.

If $p=A^2+3B^2$ with $A, B\in\mathbb{Z}$ and $A\equiv 1 \pmod 3$, from [BEW, p. 147] or [S4, (2.12)] we also have

$$2^{\frac{p-1}{3}} \equiv \begin{cases} 1 \pmod p & \text{if } B\equiv 0 \pmod 3,\\ \frac{1}{2}\big(-1-\frac{A}{B}\big) \pmod p & \text{if } B\equiv 1 \pmod 3.\end{cases}$$

Here we state the similar result for $3^{\frac{p-1}{3}} \pmod p$:

$$3^{\frac{p-1}{3}} \equiv \begin{cases} 1 \pmod p & \text{if } B\equiv 0, \pm A \pmod 9,\\ \frac{1}{2}\big(-1-\frac{A}{B}\big) \pmod p & \text{if } B\equiv 6, A+6 \pmod 9.\end{cases}$$

Theorem 4.4. *Let $p\equiv 1 \pmod 3$ be a prime. Let m be a cubefree integer with $m\not\equiv 0, \pm 1 \pmod p$ and $m\not\equiv 1 \pmod 3$. Let m_0 be the product of all distinct primes q satisfying $q\mid m$ and $q>3$. Let k_3 be given by (4.1) and $k=\frac{3+(-1)^m}{2}k_3m_0$. Then m (or $-m$) is a cubic residue of p if and only if p can be represented by some class in the set*

$$G(m)=\Big\{[a,b,c]\ \Big|\ [a,b,c]\in H(-3k^2),\ (a,6m)=1,\\ \Big(\frac{(m-1)b+k(m+1)(1+2\omega)}{a}\Big)_3=1\Big\}.$$

Moreover, $G(m)$ is a subgroup of index 3 in $H(-3k^2)$.

Proof. Let $u=(1+m)/(1+m,2)$, $v=(1-m)/(1+m,2)$ and $d=1$. From (4.2), Lemma 4.1 and Theorem 4.2 we see that $G(m)=G(u,v,d)$. Hence, it follows from Theorem 4.2 that $m^{\frac{p-1}{3}}\equiv 1 \pmod p$ if and only if p is represented by some class in $G(m)$. Moreover, $G(m)$ is a subgroup of $H(-3k^2)$. For $m=2$, clearly $k=6$ and so $|G(2)|=1=h(-3k^2)/3$. For $m\neq 2$, it is easily seen that $F(u^2-dv^2)\nmid 2u$. Thus, by Theorem 4.2 we get $|G(m)|=h(-3k^2)/3$. To complete the proof, we note that $m^{\frac{p-1}{3}}\equiv 1 \pmod p$ if and only if m is a cubic residue of p.

5. Criteria for $\varepsilon_d^{(p-(\frac{p}{3}))/3} \pmod p$.

Let $d>1$ be a squarefree integer, and let ε_d be the fundamental unit of the quadratic field $\mathbb{Q}(\sqrt{d})$. Then $\varepsilon_d=(m+n\sqrt{d})/2$ for some $m,n\in\mathbb{N}$ and $m^2-dn^2=\pm 4$. Let $p\equiv 1 \pmod 3$ be a prime such that $(\frac{d}{p})=1$. If $d\in\{2,3,5\}$, in 1973 E. Lehmer [L2] proved that ε_d is a cubic residue modulo p if and only if $p=x^2+27dy^2$ for some $x,y\in\mathbb{Z}$. In [S1], the author

gave the criteria for ε_d to be a cubic residue of p in the cases $d=6,15,21$. For a general related result one may consult [W].

When $p>3$ is a prime such that $(\frac{d}{p})=(\frac{p}{3})$, in the section we completely determine the value of $\varepsilon_d^{(p-(\frac{p}{3}))/3} \pmod p$ in terms of appropriate binary quadratic forms.

Theorem 5.1. *Suppose $m,n,d\in\mathbb{Z}$ and $m^2-dn^2=-4$. Let $p>3$ be a prime not dividing d. Let*

$$k=\begin{cases} 1 & \text{if } d\not\equiv 2 \pmod 4 \text{ and } 9\mid m,\\ 2 & \text{if } d\equiv 2 \pmod 4 \text{ and } 9\mid m,\\ 3 & \text{if } d\not\equiv 2 \pmod 4 \text{ and } 9\nmid m,\\ 6 & \text{if } d\equiv 2 \pmod 4 \text{ and } 9\nmid m. \end{cases}$$

Suppose $p=ax^2+bxy+cy^2$ with $a,b,c,x,y\in\mathbb{Z}$, $b^2-4ac=-3k^2d$ and $(a,6)=1$. If $p\nmid a$, then

$$\Big(\frac{m+n\sqrt{d}}{2}\Big)^{\frac{p-(\frac{p}{3})}{3}}$$
$$\equiv\begin{cases} (\frac{p}{3}) \pmod p & \text{if } \big(\frac{bn-km(1+2\omega)}{a}\big)_3=1,\\ \frac{1}{2}\big(-(\frac{p}{3})-\frac{2ax+by}{kdy}\sqrt{d}\big) \pmod p & \text{if } \big(\frac{bn-km(1+2\omega)}{a}\big)_3=\omega,\\ \frac{1}{2}\big(-(\frac{p}{3})+\frac{2ax+by}{kdy}\sqrt{d}\big) \pmod p & \text{if } \big(\frac{bn-km(1+2\omega)}{a}\big)_3=\omega^2. \end{cases}$$

If $p\mid a$, then

$$\Big(\frac{m+n\sqrt{d}}{2}\Big)^{\frac{p-(\frac{p}{3})}{3}}\equiv\begin{cases} (\frac{p}{3}) \pmod p & \text{if } \big(\frac{bn-km(1+2\omega)}{p}\big)_3=1,\\ \frac{1}{2}\big(-(\frac{p}{3})+\frac{b\sqrt{d}}{kd}\big) \pmod p & \text{if } \big(\frac{bn-km(1+2\omega)}{p}\big)_3=\omega,\\ \frac{1}{2}\big(-(\frac{p}{3})-\frac{b\sqrt{d}}{kd}\big) \pmod p & \text{if } \big(\frac{bn-km(1+2\omega)}{p}\big)_3=\omega^2. \end{cases}$$

Proof. Let $u=m/(m,n)$ and $v=n/(m,n)$. Since $(\frac{-4}{3})=-1$ we see that $3\nmid n$. Thus $3\nmid(m,n)$ and $3\nmid v$. Clearly $u^2-dv^2=-4/(m,n)^2$ and $d\not\equiv 3 \pmod 4$. Using Definition 3.1 we see that

$$k_2(u,v,d)=\begin{cases} 2 & \text{if } d\equiv 2 \pmod 4,\\ 1 & \text{if } d\not\equiv 2 \pmod 4, \end{cases}\quad k_3(u,v,d)=\begin{cases} 3 & \text{if } 9\nmid m,\\ 1 & \text{if } 9\mid m \end{cases}$$

and so $k(u,v,d)=k_2(u,v,d)k_3(u,v,d)=k$. Since

$$\Big(\frac{u^2-dv^2}{p}\Big)(u^2-dv^2)^{-\frac{p-(\frac{p}{3})}{6}}(u+v\sqrt{d})^{\frac{p-(\frac{p}{3})}{3}}$$
$$=\Big(\frac{-4/(m,n)^2}{p}\Big)(-4)^{-\frac{p-(\frac{p}{3})}{6}}(m,n)^{\frac{p-(\frac{p}{3})}{3}}\Big(\frac{m+n\sqrt{d}}{(m,n)}\Big)^{\frac{p-(\frac{p}{3})}{3}}$$
$$=(-1)^{\frac{p-1}{2}+\frac{p-(\frac{p}{3})}{6}}\Big(\frac{m+n\sqrt{d}}{2}\Big)^{\frac{p-(\frac{p}{3})}{3}}=\Big(\frac{p}{3}\Big)\Big(\frac{m+n\sqrt{d}}{2}\Big)^{\frac{p-(\frac{p}{3})}{3}},$$

by the above and Theorem 4.1 we obtain the result.
Remark 5.1 If $d \equiv 2 \pmod 3$, from $m^2 - dn^2 = -4$ we deduce $3 \nmid m$ and so $9 \nmid m$.

Note that $(2, 0, 27) \sim (29, -4, 2)$ and $(4, 3, 9) \sim (19, 13, 4)$. From Theorem 5.1 and the theory of reduced forms we deduce the following corollaries.

Corollary 5.1. *Let p be a prime such that $p \equiv 1, 5, 7, 11 \pmod{24}$. Then*

$$(1+\sqrt{2})^{\frac{p-1}{3}} \equiv \begin{cases} 1 \pmod p & \text{if } p = x^2 + 54y^2, \\ -\frac{1}{2} - \frac{7x+3y}{12y}\sqrt{2} \pmod p & \text{if } p = 7x^2 + 6xy + 9y^2 \neq 7, \end{cases}$$

$$(1+\sqrt{2})^{\frac{p+1}{3}} \equiv \begin{cases} -1 \pmod p & \text{if } p = 2x^2 + 27y^2, \\ \frac{1}{2} + \frac{5x+y}{12y}\sqrt{2} \pmod p & \text{if } p = 5x^2 + 2xy + 11y^2 \neq 5. \end{cases}$$

Corollary 5.2. *Let p be an odd prime such that $p \equiv 1, 2, 4, 8 \pmod{15}$. Then*

$$\left(\frac{1+\sqrt{5}}{2}\right)^{\frac{p-1}{3}} \equiv \begin{cases} 1 \pmod p & \text{if } p = x^2 + xy + 34y^2, \\ -\frac{1}{2} + \frac{38x+13y}{30y}\sqrt{5} \pmod p & \text{if } p = 19x^2 + 13xy + 4y^2 \neq 19, \end{cases}$$

$$\left(\frac{1+\sqrt{5}}{2}\right)^{\frac{p+1}{3}} \equiv \begin{cases} -1 \pmod p & \text{if } p = 5x^2 + 5xy + 8y^2, \\ \frac{1}{2} - \frac{34x+y}{30y}\sqrt{5} \pmod p & \text{if } p = 17x^2 + xy + 2y^2 \neq 17. \end{cases}$$

Corollary 5.3. *Let $p > 3$ be a prime such that $(\frac{p}{17}) = (\frac{p}{3})$. Then*

$$(4+\sqrt{17})^{\frac{p-1}{3}} \equiv \begin{cases} 1 \pmod p & \text{if } p = x^2 + xy + 115y^2, \\ -\frac{1}{2} + \frac{26x+3y}{102y}\sqrt{17} \pmod p & \text{if } p = 13x^2 + 3xy + 9y^2 \neq 13, \end{cases}$$

$$(4+\sqrt{17})^{\frac{p+1}{3}} \equiv \begin{cases} -1 \pmod p & \text{if } p = 11x^2 + 5xy + 11y^2, \\ \frac{1}{2} - \frac{10x+y}{102y}\sqrt{17} \pmod p & \text{if } p = 5x^2 + xy + 23y^2 \neq 5. \end{cases}$$

Corollary 5.4. *Let $p > 3$ be a prime such that $(\frac{p}{41}) = (\frac{p}{3})$. Then*

$$(32+5\sqrt{41})^{\frac{p-1}{3}} \equiv \begin{cases} 1 \pmod p & \text{if } p = x^2 + xy + 277y^2, \\ -\frac{1}{2} + \frac{62x+3y}{246y}\sqrt{41} \pmod p & \text{if } p = 31x^2 + 3xy + 9y^2 \neq 31, \end{cases}$$

$$(32+5\sqrt{41})^{\frac{p+1}{3}} \equiv \begin{cases} -1 \pmod p & \text{if } p = 17x^2 + 7xy + 17y^2, \\ \frac{1}{2} + \frac{22x+9y}{246y}\sqrt{41} \pmod p & \text{if } p = 11x^2 + 9xy + 27y^2 \neq 11. \end{cases}$$

Theorem 5.2. *Suppose $m, n, d \in \mathbb{Z}$ and $m^2 - dn^2 = -4$. Let $p > 3$ be a prime such that $(\frac{-3d}{p}) = 1$. Let k be as in Theorem 5.1 and*

$$S_i(m,n,d) = \Big\{ [a,b,c] \;\Big|\; [a,b,c] \in H(-3k^2d),\ a \equiv i \pmod 3,\ 2 \nmid a,\quad \Big(\frac{bn - km(1+2\omega)}{a}\Big)_3 = 1 \Big\} \quad (i = 1,2).$$

(i) *If $p \equiv 1 \pmod 3$, then $(m + n\sqrt{d})/2$ is a cubic residue of p if and only if p is represented by some class in $S_1(m,n,d)$.*

(ii) *If $p \equiv 2 \pmod 3$, then $(\frac{m+n\sqrt{d}}{2})^{\frac{p+1}{3}} \equiv -1 \pmod p$ if and only if p is represented by some class in $S_2(m,n,d)$.*

Proof. Let $u = m/(m,n)$ and $v = n/(m,n)$. Then $(u,v) = 1$, $(m,n) = 1, 2$ and $u^2 - dv^2 = -4/(m,n)^2$. From Theorem 4.1 and the proof of Theorem 5.1 we know that

$$\Big(\frac{u - v\sqrt{d}}{u + v\sqrt{d}}\Big)^{\frac{p-(\frac{p}{3})}{3}} \equiv \Big(\frac{p}{3}\Big)\Big(\frac{m + n\sqrt{d}}{2}\Big)^{\frac{p-(\frac{p}{3})}{3}} \pmod p.$$

By the proof of Theorem 5.1 we have $k = k(u,v,d)$. Hence applying the above and Theorem 4.2 we see that $\big(\frac{m+n\sqrt{d}}{2}\big)^{\frac{p-(\frac{p}{3})}{3}} \equiv \big(\frac{p}{3}\big) \pmod p$ if and only if p is represented by some class in the set

$$G(u,v,d) = \Big\{ [a,b,c] \;\Big|\; [a,b,c] \in H(-3k^2d),\ (a,6) = 1,\ \Big(\frac{bn - km(1+2\omega)}{a}\Big)_3 = 1 \Big\}.$$

Clearly $G(u,v,d) = S_1(m,n,d) \cup S_2(m,n,d)$.

Since $(\frac{-3k^2d}{p}) = (\frac{-3d}{p}) = 1$, p can be represented by some class in $H(-3k^2d)$. Suppose $p = ax^2 + bxy + cy^2$ with $a, b, c, x, y \in \mathbb{Z}$, $(a,6) = 1$ and $b^2 - 4ac = -3k^2d$. As $4ap = (2ax + by)^2 + 3k^2dy^2$ and $3 \nmid ap$, we see that $ap \equiv 1 \pmod 3$ and so $p \equiv a \pmod 3$. Now combining the above with Euler's criterion we obtain the result.

Theorem 5.3. *Suppose $m, n, d \in \mathbb{Z}$, $dn \neq 0$ and $m^2 - dn^2 = 4$. Let $p > 3$ be a prime not dividing d. Let*

$$k = \begin{cases} 1 & \text{if } d \equiv 0,1 \pmod 4 \text{ and } 9 \mid m, \\ 2 & \text{if } d \equiv 2,3 \pmod 4 \text{ and } 9 \mid m, \\ 3^{\mathrm{ord}_3 n + 1} & \text{if } d \equiv 0,1 \pmod 4 \text{ and } 9 \nmid m, \\ 2 \cdot 3^{\mathrm{ord}_3 n + 1} & \text{if } d \equiv 2,3 \pmod 4 \text{ and } 9 \nmid m. \end{cases}$$

Suppose $p = ax^2 + bxy + cy^2$ *with* $a, b, c, x, y \in \mathbb{Z}$, $b^2 - 4ac = -3k^2d$ *and* $(a, 6) = 1$. *If* $p \nmid a$, *then*

$$\Big(\frac{m+n\sqrt{d}}{2}\Big)^{\frac{p-(\frac{p}{3})}{3}} \equiv \begin{cases} 1 \pmod p & \text{if } \big(\frac{bn-km(1+2\omega)}{a}\big)_3 = 1, \\ -\frac{1}{2}\big(1 + (\frac{p}{3})\frac{2ax+by}{kdy}\sqrt{d}\big) \pmod p & \text{if } \big(\frac{bn-km(1+2\omega)}{a}\big)_3 = \omega, \\ \frac{1}{2}\big(-1 + (\frac{p}{3})\frac{2ax+by}{kdy}\sqrt{d}\big) \pmod p & \text{if } \big(\frac{bn-km(1+2\omega)}{a}\big)_3 = \omega^2. \end{cases}$$

If $p \mid a$, *then*

$$\Big(\frac{m+n\sqrt{d}}{2}\Big)^{\frac{p-(\frac{p}{3})}{3}} \equiv \begin{cases} 1 \pmod p & \text{if } \big(\frac{bn-km(1+2\omega)}{p}\big)_3 = 1, \\ \frac{1}{2}\big(-1 + (\frac{p}{3})\frac{b\sqrt{d}}{kd}\big) \pmod p & \text{if } \big(\frac{bn-km(1+2\omega)}{p}\big)_3 = \omega, \\ \frac{1}{2}\big(-1 - (\frac{p}{3})\frac{b\sqrt{d}}{kd}\big) \pmod p & \text{if } \big(\frac{bn-km(1+2\omega)}{p}\big)_3 = \omega^2. \end{cases}$$

Proof. Let $u = m/(m,n)$ and $v = n/(m,n)$. Then $(u,v) = 1$ and $u^2 - dv^2 = 4/(m,n)^2$. One can easily show that

$$k = k(u,v,d) \quad \text{and} \quad \Big(\frac{u-v\sqrt{d}}{u+v\sqrt{d}}\Big)^{\frac{p-(\frac{p}{3})}{3}} \equiv \Big(\frac{m+n\sqrt{d}}{2}\Big)^{\frac{p-(\frac{p}{3})}{3}} \pmod p.$$

Thus applying Theorem 4.1 we obtain the result.

Remark 5.2 If $d \equiv 0, 1 \pmod 3$ and $m^2 - dn^2 = 4$ with $m, n, d \in \mathbb{Z}$, we must have $3 \nmid m$ and so $9 \nmid m$.

Observe that $(2, 0, 81) \sim (83, -4, 2)$ and $(9, 6, 10) \sim (13, 12, 9)$. From Theorem 5.3 and the theory of reduced forms we have the following results.

Corollary 5.5. *Let* $p \equiv 1 \pmod 4$ *be a prime. Then*

$$(2+\sqrt{3})^{\frac{p-(\frac{p}{3})}{3}} \equiv \begin{cases} 1 \pmod p & \text{if } p = x^2 + 81y^2,\ 2x^2 + 2xy + 41y^2, \\ -\frac{1}{2} + \frac{13x+6y}{18y}\sqrt{3} \pmod p & \text{if } p = 13x^2 + 12xy + 9y^2 \neq 13, \\ -\frac{1}{2} - \frac{5x+2y}{18y}\sqrt{3} \pmod p & \text{if } p = 5x^2 + 4xy + 17y^2 \neq 5. \end{cases}$$

Corollary 5.6. *Let* $p > 3$ *be a prime such that* $p \equiv 1, 3 \pmod 8$. *Then*

$$(5+2\sqrt{6})^{\frac{p-(\frac{p}{3})}{3}} \equiv \begin{cases} 1 \pmod p & \text{if } p = x^2 + 162y^2,\ 2x^2 + 81y^2, \\ -\frac{1}{2} - \frac{19x+3y}{36y}\sqrt{6} \pmod p & \text{if } p = 19x^2 + 6xy + 9y^2 \neq 19, \\ -\frac{1}{2} + \frac{11x+5y}{36y}\sqrt{6} \pmod p & \text{if } p = 11x^2 + 10xy + 17y^2 \neq 11. \end{cases}$$

From Theorems 4.2, 5.3 and the proofs of Theorems 5.2 and 5.3 we have the following theorem.

Theorem 5.4. *Suppose $m, n, d \in \mathbb{Z}$, $dn \neq 0$ and $m^2 - dn^2 = 4$. Let $p > 3$ be a prime such that $(\frac{-3d}{p}) = 1$. Let k be as in Theorem 5.3 and*

$$T_i(m,n,d) = \Big\{ [a,b,c] \;\Big|\; [a,b,c] \in H(-3k^2d),\ a \equiv i \pmod 3,$$
$$2 \nmid a, \quad \Big(\frac{bn - km(1+2\omega)}{a}\Big)_3 = 1 \Big\} \quad (i = 1, 2).$$

(i) *If $p \equiv 1 \pmod 3$, then $(m + n\sqrt{d})/2$ is a cubic residue of p if and only if p is represented by some class in $T_1(m, n, d)$.*

(ii) *If $p \equiv 2 \pmod 3$, then $(\frac{m+n\sqrt{d}}{2})^{\frac{p+1}{3}} \equiv 1 \pmod p$ if and only if p is represented by some class in $T_2(m, n, d)$.*

If $m, n, d \in \mathbb{Z}$ with $m^2 - dn^2 = 4$ and $dn \neq 0$, then clearly $(m-2)(m+2) = dn^2$ and so $\operatorname{ord}_3(m-2) + \operatorname{ord}_3(m+2) \geq 2\ \operatorname{ord}_3 n$. Hence $\operatorname{ord}_3(m-2) \geq \operatorname{ord}_3 n$ or $\operatorname{ord}_3(m+2) \geq \operatorname{ord}_3 n$. Thus we may choose the sign of m such that $\operatorname{ord}_3(m-2) \geq \operatorname{ord}_3 n$.

Theorem 5.5. *Suppose $m, n, d \in \mathbb{Z}$, $m^2 - dn^2 = 4$ and $\operatorname{ord}_3(m-2) \geq \operatorname{ord}_3 n$. Let $p > 3$ be a prime such that $p \nmid dn$. Let $2^\alpha \parallel \frac{4(m-2)}{(m-2,n)^2}$. Let*

$$k_2 = \begin{cases} 2 & \text{if } d \equiv 2, 3 \pmod 4, \\ 2 & \text{if } d \equiv 1 \pmod 8,\ \alpha > 0 \text{ and } \alpha \equiv 0, 1 \pmod 3, \\ 1 & \text{otherwise,} \end{cases}$$

$$k_3 = \begin{cases} 3 & \text{if } 9 \nmid \frac{m-2}{(m-2,n)}, \\ 1 & \text{if } 9 \mid \frac{m-2}{(m-2,n)} \end{cases} \quad \text{and} \quad k = k_2 k_3.$$

Suppose $p = ax^2 + bxy + cy^2$ with $a, b, c, x, y \in \mathbb{Z}$, $b^2 - 4ac = -3k^2d$ and $(a, 6(8-4m)/(m-2,n)^2) = 1$. If $p \nmid a$, then

$$\Big(\frac{m+n\sqrt{d}}{2}\Big)^{\frac{p-(\frac{p}{3})}{3}}$$
$$\equiv \begin{cases} 1 \pmod p & \text{if } \Big(\frac{\frac{bn}{(m-2,n)} + \frac{k(m-2)}{(m-2,n)}(1+2\omega)}{a}\Big)_3 = 1, \\ \frac{1}{2}\big(-1 - (\frac{p}{3})\frac{2ax+by}{kdy}\sqrt{d}\big) \pmod p & \text{if } \Big(\frac{\frac{bn}{(m-2,n)} + \frac{k(m-2)}{(m-2,n)}(1+2\omega)}{a}\Big)_3 = \omega, \\ \frac{1}{2}\big(-1 + (\frac{p}{3})\frac{2ax+by}{kdy}\sqrt{d}\big) \pmod p & \text{if } \Big(\frac{\frac{bn}{(m-2,n)} + \frac{k(m-2)}{(m-2,n)}(1+2\omega)}{a}\Big)_3 = \omega^2. \end{cases}$$

If $p \mid a$, then

$$\Big(\frac{m+n\sqrt{d}}{2}\Big)^{\frac{p-(\frac{p}{3})}{3}}$$
$$\equiv \begin{cases} 1 \pmod p & \text{if } \Big(\frac{\frac{bn}{(m-2,n)} + \frac{k(m-2)}{(m-2,n)}(1+2\omega)}{p}\Big)_3 = 1, \\ \frac{1}{2}\big(-1 + (\frac{p}{3})\frac{b\sqrt{d}}{kd}\big) \pmod p & \text{if } \Big(\frac{\frac{bn}{(m-2,n)} + \frac{k(m-2)}{(m-2,n)}(1+2\omega)}{p}\Big)_3 = \omega, \\ \frac{1}{2}\big(-1 - (\frac{p}{3})\frac{b\sqrt{d}}{kd}\big) \pmod p & \text{if } \Big(\frac{\frac{bn}{(m-2,n)} + \frac{k(m-2)}{(m-2,n)}(1+2\omega)}{p}\Big)_3 = \omega^2. \end{cases}$$

Proof. Let $u=(2-m)/(m-2,n)$ and $v=n/(m-2,n)$. Then $(u,v)=1$, $3\nmid v$ and $u^2-dv^2=4(2-m)/(m-2,n)^2$. Since $\mathrm{ord}_3(u^2-dv^2)=\mathrm{ord}_3u-\mathrm{ord}_3n$, using Definition 3.1 we see that $k_2(u,v,d)=k_2$, $k_3(u,v,d)=k_3$ and so $k(u,v,d)=k_2(u,v,d)k_3(u,v,d)=k_2k_3=k$. It is easy to see that

$$\frac{m+n\sqrt{d}}{2}=-\frac{u-v\sqrt{d}}{u+v\sqrt{d}}\quad\text{and so}\quad\Big(\frac{m+n\sqrt{d}}{2}\Big)^{\frac{p-(\frac{p}{3})}{3}}=\Big(\frac{u-v\sqrt{d}}{u+v\sqrt{d}}\Big)^{\frac{p-(\frac{p}{3})}{3}}.$$

Now the result follows from the above and Theorem 4.1.

As an example, putting $d=7$, $m=-16$ and $n=-6$ in Theorem 5.5 and noting that $(25,12,9)\sim(9,6,22)$ we deduce the following corollary.

Corollary 5.7. *Let $p>3$ be a prime.*

(i) *If $p\equiv 1\pmod 3$ and $(\frac{7}{p})=1$, then*

$$(8+3\sqrt{7})^{\frac{p-1}{3}}\equiv\begin{cases}1\pmod p & \text{if } p=x^2+189y^2,\ 7x^2+27y^2,\\ -\frac12-\frac{19x+y}{42y}\sqrt{7}\pmod p & \text{if } p=19x^2+2xy+10y^2\neq 19,\\ -\frac12-\frac{25x+6y}{42y}\sqrt{7}\pmod p & \text{if } p=25x^2+12xy+9y^2.\end{cases}$$

(ii) *If $p\equiv 2\pmod 3$ and $(\frac{7}{p})=-1$, then*

$$(8+3\sqrt{7})^{\frac{p+1}{3}}\equiv\begin{cases}1\pmod p & \text{if } p=2x^2+2xy+95y^2\\ & \quad \text{or } 14x^2+14xy+17y^2,\\ -\frac12-\frac{5x+y}{42y}\sqrt{7}\pmod p & \text{if } p=5x^2+2xy+38y^2\neq 5,\\ -\frac12-\frac{11x+3y}{42y}\sqrt{7}\pmod p & \text{if } p=11x^2+6xy+18y^2\neq 11.\end{cases}$$

If $m^2-dn^2=4$ with $m,n,d\in\mathbb{Z}$, then $\frac{m+n\sqrt{d}}{2}\cdot\frac{-m+n\sqrt{d}}{2}=-1$. Thus for any prime $p>3$,

$$\Big(\frac{m+n\sqrt{d}}{2}\Big)^{\frac{p-(\frac{p}{3})}{3}}\equiv 1\pmod p\iff\Big(\frac{-m+n\sqrt{d}}{2}\Big)^{\frac{p-(\frac{p}{3})}{3}}\equiv 1\pmod p.$$

Now from Theorem 4.2 and the proof of Theorem 5.5 we deduce the following result.

Theorem 5.6. *Suppose $m,n,d\in\mathbb{Z}$, $m^2-dn^2=4$ and $\mathrm{ord}_3(m-2)\geq\mathrm{ord}_3n$. Let $p>3$ be a prime such that $p\nmid dn$ and $(\frac{-3d}{p})=1$. Let k be given as in Theorem 5.5. Then $\big(\frac{\pm m+n\sqrt{d}}{2}\big)^{(p-(\frac{p}{3}))/3}\equiv 1\pmod p$ if and only if p is represented by some class in the set*

$$L(m,n,d)=\Big\{[a,b,c]\ \Big|\ [a,b,c]\in H(-3k^2d),\ \Big(a,\frac{6(8-4m)}{(m-2,n)^2}\Big)=1,\ \Big(\frac{\frac{bn}{(m-2,n)}+\frac{k(m-2)}{(m-2,n)}(1+2\omega)}{a}\Big)_3=1\Big\}.$$

Moreover, $L(m,n,d)$ is a subgroup of $H(-3k^2d)$.

6. Applications to Lucas sequences.

For $P, Q \in \mathbb{Z}$ and an odd prime p with $(\frac{-3(P^2-4Q)}{p}) = 1$, in the section we will determine $U_{(p-(\frac{p}{3}))/3}(P,Q)$ and $V_{(p-(\frac{p}{3}))/3}(P,Q)$ modulo p, where $U_n(P,Q)$ and $V_n(P,Q)$ are the Lucas sequences given by

$$U_0(P,Q) = 0,\ U_1(P,Q) = 1,\ U_{n+1}(P,Q) = PU_n(P,Q) - QU_{n-1}(P,Q)(n \ge 1)$$

and

$$V_0(P,Q) = 2,\ V_1(P,Q) = P,\ V_{n+1}(P,Q) = PV_n(P,Q) - QV_{n-1}(P,Q)(n \ge 1).$$

It is well known that

(6.1)
$$U_n(P,Q) = \begin{cases} \frac{1}{\sqrt{P^2-4Q}}\{(\frac{P+\sqrt{P^2-4Q}}{2})^n - (\frac{P-\sqrt{P^2-4Q}}{2})^n\} & \text{if } P^2-4Q \neq 0, \\ n(\frac{P}{2})^{n-1} & \text{if } P^2-4Q = 0 \end{cases}$$

and

$$V_n(P,Q) = \Big(\frac{P+\sqrt{P^2-4Q}}{2}\Big)^n + \Big(\frac{P-\sqrt{P^2-4Q}}{2}\Big)^n. \tag{6.2}$$

Theorem 6.1. *Let $p > 3$ be a prime, and $P, Q \in \mathbb{Z}$ with $p \nmid Q$ and $(\frac{-3(P^2-4Q)}{p}) = 1$. Assume $P^2-4Q = df^2$ $(d, f \in \mathbb{Z})$ and $p = ax^2+bxy+cy^2$ with $a, b, c, x, y \in \mathbb{Z}$, $(a, 6p \cdot 4Q/(P,f)^2) = 1$ and $b^2-4ac = -3k^2d$, where $k = k(P/(P,f), f/(P,f), d)$. Then*

$$U_{(p-(\frac{p}{3}))/3}(P,Q)$$
$$\equiv \begin{cases} 0 \pmod p & \text{if } \Big(\frac{\frac{bf}{(P,f)} - \frac{kP}{(P,f)}(1+2\omega)}{a}\Big)_3 = 1, \\ -\frac{2ax+by}{kdfy}(\frac{-Q}{p})(-Q)^{\frac{p-(\frac{p}{3})}{6}} \pmod p & \text{if } \Big(\frac{\frac{bf}{(P,f)} - \frac{kP}{(P,f)}(1+2\omega)}{a}\Big)_3 = \omega, \\ \frac{2ax+by}{kdfy}(\frac{-Q}{p})(-Q)^{\frac{p-(\frac{p}{3})}{6}} \pmod p & \text{if } \Big(\frac{\frac{bf}{(P,f)} - \frac{kP}{(P,f)}(1+2\omega)}{a}\Big)_3 = \omega^2 \end{cases}$$

and

$$V_{(p-(\frac{p}{3}))/3}(P,Q)$$
$$\equiv \begin{cases} 2(\frac{p}{3})(\frac{-Q}{p})(-Q)^{\frac{p-(\frac{p}{3})}{6}} \pmod p & \text{if } \Big(\frac{\frac{bf}{(P,f)} - \frac{kP}{(P,f)}(1+2\omega)}{a}\Big)_3 = 1, \\ -(\frac{p}{3})(\frac{-Q}{p})(-Q)^{\frac{p-(\frac{p}{3})}{6}} \pmod p & \text{if } \Big(\frac{\frac{bf}{(P,f)} - \frac{kP}{(P,f)}(1+2\omega)}{a}\Big)_3 \neq 1. \end{cases}$$

Proof. Since $p \nmid aQ$ and $(a,y) \mid p$ we see that $p \nmid ky$ and $(a,y) = 1$. Let $u = P/(P,f)$ and $v = f/(P,f)$. Then $(u,v) = 1$ and $u^2-dv^2 = 4Q/(P,f)^2$. For $n \in \mathbb{N}$ it is clear that

$$\Big(\frac{u^2-dv^2}{p}\Big)(u^2-dv^2)^{-n}(u \pm v\sqrt{d})^{2n} = \Big(\frac{Q}{p}\Big)Q^{-n}\Big(\frac{P \pm f\sqrt{d}}{2}\Big)^{2n}.$$

Thus applying (6.1) and (6.2) we see that

$$\Big(\frac{u^2-dv^2}{p}\Big)(u^2-dv^2)^{-n}\Big\{(u+v\sqrt{d})^{2n}-(u-v\sqrt{d})^{2n}\Big\}$$
$$=\Big(\frac{Q}{p}\Big)Q^{-n}f\sqrt{d}U_{2n}(P,Q)$$

and

$$\Big(\frac{u^2-dv^2}{p}\Big)(u^2-dv^2)^{-n}\Big\{(u+v\sqrt{d})^{2n}+(u-v\sqrt{d})^{2n}\Big\}$$
$$=\Big(\frac{Q}{p}\Big)Q^{-n}V_{2n}(P,Q).$$

Now set $n=(p-(\frac{p}{3}))/6$. If $\big(\frac{bv-ku(1+2\omega)}{a}\big)_3=1$, then $\big(\frac{b(-v)-ku(1+2\omega)}{a}\big)_3=1$. Observe that $k(u,v,d)=k(u,-v,d)$. By the above and Theorem 4.1 we have $(\frac{Q}{p})Q^{-n}f\sqrt{d}U_{2n}(P,Q)\equiv 1-1=0 \pmod p$ and $(\frac{Q}{p})Q^{-n}V_{2n}(P,Q)\equiv 1+1=2 \pmod p$. Thus

$$p\mid U_{2n}(P,Q) \quad\text{and}\quad V_{2n}(P,Q)\equiv 2\Big(\frac{Q}{p}\Big)Q^n \pmod p.$$

If $\big(\frac{bv-ku(1+2\omega)}{a}\big)_3=\omega^{\pm1}$, then $\big(\frac{b(-v)-ku(1+2\omega)}{a}\big)_3=\omega^{\mp1}$. From the above and Theorem 4.1 we have

$$\Big(\frac{Q}{p}\Big)Q^{-n}f\sqrt{d}U_{2n}(P,Q)\equiv\frac{-1\mp(\frac{p}{3})\frac{2ax+by}{kdy}\sqrt{d}}{2}-\frac{-1\pm(\frac{p}{3})\frac{2ax+by}{kdy}\sqrt{d}}{2}$$
$$=\mp\Big(\frac{p}{3}\Big)\frac{2ax+by}{kdy}\sqrt{d} \pmod p$$

and

$$\Big(\frac{Q}{p}\Big)Q^{-n}V_{2n}(P,Q)\equiv\frac{-1\mp(\frac{p}{3})\frac{2ax+by}{kdy}\sqrt{d}}{2}+\frac{-1\pm(\frac{p}{3})\frac{2ax+by}{kdy}\sqrt{d}}{2}$$
$$=-1 \pmod p.$$

Thus

$$U_{2n}(P,Q)\equiv\mp\Big(\frac{p}{3}\Big)\Big(\frac{Q}{p}\Big)Q^n\frac{2ax+by}{kdfy} \pmod p$$

and

$$V_{2n}(P,Q)\equiv-\Big(\frac{Q}{p}\Big)Q^n \pmod p.$$

To complete the proof, we note that $\big(\frac{-1}{p}\big)\cdot(-1)^n=\big(\frac{-1}{p}\big)\big(\frac{3}{p}\big)=\big(\frac{-3}{p}\big)=\big(\frac{p}{3}\big)$.

Remark 6.1 According to (6.1), (6.2) and Theorem 4.1, the criteria for

$p \mid U_{(p-(\frac{p}{3}))/3}(P,Q)$ and $V_{(p-(\frac{p}{3}))/3}(P,Q) \pmod p$ in Theorem 6.1 are also true when $p = a$.

If $p \nmid Q$ and $(\frac{-3(P^2-4Q)}{p}) = -1$, from [S2, Theorem 2.1] we know that

$$U_{\frac{p-(\frac{p}{3})}{3}}(P,Q) \equiv \frac{1}{P^2-4Q}\Big(\frac{-3Q}{p}\Big)Q^{\frac{p-(\frac{p}{3})}{6}-1}(-Px^2+2Qx+2PQ) \pmod p$$

and

$$V_{\frac{p-(\frac{p}{3})}{3}}(P,Q) \equiv \Big(\frac{Q}{p}\Big)Q^{\frac{p-(\frac{p}{3})}{6}-1}(x^2-2Q) \pmod p,$$

where x is the unique solution of the congruence $X^3 - 3QX - PQ \equiv 0 \pmod p$.

Putting $P = 6$, $Q = 3m+9$, $d = -3m$ and $f = 2$ in Theorem 6.1 we deduce the following result.

Corollary 6.1. *Let $p > 3$ be a prime, and $m \in \mathbb{Z}$ with $p \nmid m+3$ and $(\frac{m}{p}) = 1$. Assume $p = ax^2+bxy+cy^2$ with $a, b, c, x, y \in \mathbb{Z}$, $(a, 6p(m+3)) = 1$ and $b^2 - 4ac = 9k^2m$, where $k = k(3, 1, -3m)$. Then*

$$U_{(p-(\frac{p}{3}))/3}(6, 3m+9)$$
$$\equiv \begin{cases} 0 \pmod p & \text{if } \big(\frac{b-3k(1+2\omega)}{a}\big)_3 = 1, \\ \frac{2ax+by}{6kmy}(\frac{-3m-9}{p})(-3m-9)^{\frac{p-(\frac{p}{3})}{6}} \pmod p & \text{if } \big(\frac{b-3k(1+2\omega)}{a}\big)_3 = \omega, \\ -\frac{2ax+by}{6kmy}(\frac{-3m-9}{p})(-3m-9)^{\frac{p-(\frac{p}{3})}{6}} \pmod p & \text{if } \big(\frac{b-3k(1+2\omega)}{a}\big)_3 = \omega^2 \end{cases}$$

and

$$V_{(p-(\frac{p}{3}))/3}(6, 3m+9)$$
$$\equiv \begin{cases} 2(\frac{p}{3})(\frac{-3m-9}{p})(-3m-9)^{\frac{p-(\frac{p}{3})}{6}} \pmod p & \text{if } \big(\frac{b-3k(1+2\omega)}{a}\big)_3 = 1, \\ -(\frac{p}{3})(\frac{-3m-9}{p})(-3m-9)^{\frac{p-(\frac{p}{3})}{6}} \pmod p & \text{if } \big(\frac{b-3k(1+2\omega)}{a}\big)_3 \neq 1. \end{cases}$$

If $m, n, d \in \mathbb{Z}$ and $m^2 + 4 = dn^2$, from (6.1) and (6.2) we have

$$U_r(m,-1) = \frac{1}{n\sqrt{d}}\Big\{\Big(\frac{m+n\sqrt{d}}{2}\Big)^r - \Big(\frac{m-n\sqrt{d}}{2}\Big)^r\Big\},$$
$$V_r(m,-1) = \Big(\frac{m+n\sqrt{d}}{2}\Big)^r + \Big(\frac{m-n\sqrt{d}}{2}\Big)^r.$$

Thus applying Theorem 5.1 or Theorem 6.1 we deduce the following result.

Corollary 6.2. *Suppose $d, m, n \in \mathbb{Z}$ and $m^2+4 = dn^2$. Let $p > 3$ be a prime such that $p \nmid m^2+4$ and $(\frac{-3d}{p}) = 1$. Let k be as in Theorem 5.1. Suppose $p = ax^2+bxy+cy^2$ with $a, b, c, x, y \in \mathbb{Z}$, $b^2-4ac = -3k^2d$ and $(a, 6p) = 1$. Then*

$$U_{\frac{p-(\frac{p}{3})}{3}}(m,-1) \equiv \begin{cases} 0 \pmod p & \text{if } \left(\frac{bn-km(1+2\omega)}{a}\right)_3 = 1, \\ -\frac{2ax+by}{kdny} \pmod p & \text{if } \left(\frac{bn-km(1+2\omega)}{a}\right)_3 = \omega, \\ \frac{2ax+by}{kdny} \pmod p & \text{if } \left(\frac{bn-km(1+2\omega)}{a}\right)_3 = \omega^2 \end{cases}$$

and

$$V_{\frac{p-(\frac{p}{3})}{3}}(m,-1) \equiv \begin{cases} 2(\frac{p}{3}) \pmod p & \text{if } \left(\frac{bn-km(1+2\omega)}{a}\right)_3 = 1, \\ -(\frac{p}{3}) \pmod p & \text{if } \left(\frac{bn-km(1+2\omega)}{a}\right)_3 = \omega, \omega^2. \end{cases}$$

From (6.1), (6.2) and Corollaries 5.6, 5.7, 5.3, 5.4 (or Theorem 6.1) we have the following four corollaries.

Corollary 6.3. *Let $p > 3$ be a prime such that $p \equiv 1, 3 \pmod 8$. Then*

$$U_{\frac{p-(\frac{p}{3})}{3}}(10,1) \equiv \begin{cases} 0 \pmod p & \text{if } p = x^2+162y^2,\ 2x^2+81y^2, \\ -\frac{19x+3y}{72y} \pmod p & \text{if } p = 19x^2+6xy+9y^2 \neq 19, \\ \frac{11x+5y}{72y} \pmod p & \text{if } p = 11x^2+10xy+17y^2 \neq 11 \end{cases}$$

and

$$V_{\frac{p-(\frac{p}{3})}{3}}(10,1) \equiv \begin{cases} 2 \pmod p & \text{if } p = x^2+162y^2,\ 2x^2+81y^2, \\ -1 \pmod p & \text{otherwise.} \end{cases}$$

Corollary 6.4. *Let $p > 3$ be a prime.*

(i) *If $p \equiv 1 \pmod 3$ and $(\frac{7}{p}) = 1$, then*

$$U_{\frac{p-1}{3}}(16,1) \equiv \begin{cases} 0 \pmod p & \text{if } p = x^2+189y^2,\ 7x^2+27y^2, \\ -\frac{19x+y}{126y} \pmod p & \text{if } p = 19x^2+2xy+10y^2 \neq 19, \\ -\frac{25x+6y}{126y} \pmod p & \text{if } p = 25x^2+12xy+9y^2 \end{cases}$$

and

$$V_{\frac{p-1}{3}}(16,1) \equiv \begin{cases} 2 \pmod p & \text{if } p = x^2+189y^2,\ 7x^2+27y^2, \\ -1 \pmod p & \text{otherwise.} \end{cases}$$

(ii) *If $p \equiv 2 \pmod 3$ and $(\frac{7}{p}) = -1$, then*

$$U_{\frac{p+1}{3}}(16,1) \equiv \begin{cases} 0 \pmod p & \text{if } p = 2x^2+2xy+95y^2 \\ & \quad \text{or } 14x^2+14xy+17y^2, \\ -\frac{5x+y}{126y} \pmod p & \text{if } p = 5x^2+2xy+38y^2 \neq 5, \\ -\frac{11x+3y}{126y} \pmod p & \text{if } p = 11x^2+6xy+18y^2 \neq 11 \end{cases}$$

and

$$V_{\frac{p+1}{3}}(16,1) \equiv \begin{cases} 2 \pmod{p} & \text{if } p = 2x^2+2xy+95y^2 \\ & \quad \text{or } 14x^2+14xy+17y^2, \\ -1 \pmod{p} & \text{otherwise.} \end{cases}$$

Corollary 6.5. *Let p be a prime greater than 3 such that $(\frac{p}{17}) = (\frac{p}{3})$. Then*

$$U_{\frac{p-(\frac{p}{3})}{3}}(8,-1) \equiv \begin{cases} 0 \pmod{p} & \text{if } p = x^2+xy+115y^2 \\ & \quad \text{or } p = 11x^2+5xy+11y^2, \\ \frac{26x+3y}{102y} \pmod{p} & \text{if } p = 13x^2+3xy+9y^2 \neq 13, \\ -\frac{10x+y}{102y} \pmod{p} & \text{if } p = 5x^2+xy+23y^2 \neq 5 \end{cases}$$

and

$$V_{\frac{p-(\frac{p}{3})}{3}}(8,-1) \equiv \begin{cases} 2 \pmod{p} & \text{if } p = x^2+xy+115y^2, \\ -2 \pmod{p} & \text{if } p = 11x^2+5xy+11y^2, \\ -1 \pmod{p} & \text{if } p = 13x^2+3xy+9y^2, \\ 1 \pmod{p} & \text{if } p = 5x^2+xy+23y^2. \end{cases}$$

Corollary 6.6. *Let p be a prime greater than 3 such that $(\frac{p}{41}) = (\frac{p}{3})$. Then*

$$U_{\frac{p-(\frac{p}{3})}{3}}(64,-1) \equiv \begin{cases} 0 \pmod{p} & \text{if } p = x^2+xy+277y^2 \\ & \quad \text{or } p = 17x^2+7xy+17y^2, \\ \frac{62x+3y}{1230y} \pmod{p} & \text{if } p = 31x^2+3xy+9y^2 \neq 31, \\ \frac{22x+9y}{1230y} \pmod{p} & \text{if } p = 11x^2+9xy+27y^2 \neq 11 \end{cases}$$

and

$$V_{\frac{p-(\frac{p}{3})}{3}}(64,-1) \equiv \begin{cases} 2 \pmod{p} & \text{if } p = x^2+xy+277y^2, \\ -2 \pmod{p} & \text{if } p = 17x^2+7xy+17y^2, \\ -1 \pmod{p} & \text{if } p = 31x^2+3xy+9y^2, \\ 1 \pmod{p} & \text{if } p = 11x^2+9xy+27y^2. \end{cases}$$

Putting $m = 3$, $n = 1$, $d = 13$ and $k = 3$ in Corollary 6.2 and observing that $(10,7,10) \sim (13,13,10)$, $(25,7,4) \sim (4,1,22)$, $(43,37,10) \sim (9,-3,10)$ and $(47,5,2) \sim (2,-1,44)$ we deduce the following result.

Corollary 6.7. *Let $p > 3$ be a prime.*

(i) *If* $p \equiv 1 \pmod 3$ *and* $(\frac{p}{13}) = 1$, *then*

$$U_{\frac{p-1}{3}}(3,-1) \equiv \begin{cases} 0 \pmod p & \text{if } p = x^2 + xy + 88y^2 \\ & \quad \text{or } p = 10x^2 + 7xy + 10y^2, \\ \frac{50x+7y}{39y} \pmod p & \text{if } p = 25x^2 + 7xy + 4y^2, \\ -\frac{86x+37y}{39y} \pmod p & \text{if } p = 43x^2 + 37xy + 10y^2 \neq 43 \end{cases}$$

and

$$V_{\frac{p-1}{3}}(3,-1) \equiv \begin{cases} 2 \pmod p & \text{if } p = x^2 + xy + 88y^2 \\ & \quad \text{or } p = 10x^2 + 7xy + 10y^2, \\ -1 \pmod p & \text{otherwise.} \end{cases}$$

(ii) *If* $p \equiv 2 \pmod 3$ *and* $(\frac{p}{13}) = -1$, *then*

$$U_{\frac{p+1}{3}}(3,-1) \equiv \begin{cases} 0 \pmod p & \text{if } p = 11x^2 + xy + 8y^2, \\ \frac{10x+3y}{39y} \pmod p & \text{if } p = 5x^2 + 3xy + 18y^2 \neq 5, \\ \frac{94x+5y}{39y} \pmod p & \text{if } p = 47x^2 + 5xy + 2y^2 \neq 47 \end{cases}$$

and

$$V_{\frac{p+1}{3}}(3,-1) \equiv \begin{cases} -2 \pmod p & \text{if } p = 11x^2 + xy + 8y^2, \\ 1 \pmod p & \text{otherwise.} \end{cases}$$

From Corollary 6.2 we also deduce the following results.

Corollary 6.8. *Let* $p > 5$ *be a prime such that* $(\frac{-30}{p}) = 1$.

(i) *If* $p \equiv 1 \pmod 3$, *then*

$$U_{\frac{p-1}{3}}(6,-1) \equiv \begin{cases} 0 \pmod p & \text{if } p = x^2 + 270y^2,\ 10x^2 + 27y^2, \\ -\frac{31x+3y}{60y} \pmod p & \text{if } p = 31x^2 + 6xy + 9y^2 \neq 31, \\ -\frac{13x+4y}{60y} \pmod p & \text{if } p = 13x^2 + 8xy + 22y^2 \neq 13 \end{cases}$$

and

$$V_{\frac{p-1}{3}}(6,-1) \equiv \begin{cases} 2 \pmod p & \text{if } p = x^2 + 270y^2,\ 10x^2 + 27y^2, \\ -1 \pmod p & \text{otherwise.} \end{cases}$$

(ii) *If* $p \equiv 2 \pmod 3$, *then*

$$U_{\frac{p+1}{3}}(6,-1) \equiv \begin{cases} 0 \pmod p & \text{if } p = 2x^2 + 135y^2,\ 5x^2 + 54y^2, \\ \frac{11x+4y}{60y} \pmod p & \text{if } p = 11x^2 + 8xy + 26y^2 \neq 11, \\ \frac{17x+6y}{60y} \pmod p & \text{if } p = 17x^2 + 12xy + 18y^2 \neq 17 \end{cases}$$

and

$$V_{\frac{p+1}{3}}(6,-1) \equiv \begin{cases} -2 \pmod p & \text{if } p = 2x^2 + 135y^2,\ 5x^2 + 54y^2, \\ 1 \pmod p & \text{otherwise.} \end{cases}$$

Corollary 6.9. *Let $p>3$ be a prime such that $(\frac{p}{5})(\frac{p}{17})=(\frac{p}{3})$.*

(i) *If $p\equiv 1 \pmod 3$, then*

$$U_{\frac{p-1}{3}}(9,-1)\equiv\begin{cases} 0 \pmod p & \text{if } p=x^2+xy+64y^2 \\ & \quad \text{or } p=3x^2+3xy+22y^2, \\ \frac{38x+7y}{85y} \pmod p & \text{if } p=19x^2+7xy+4y^2\neq 19, \\ \frac{14x+5y}{85y} \pmod p & \text{if } p=7x^2+5xy+10y^2\neq 7 \end{cases}$$

and

$$V_{\frac{p-1}{3}}(9,-1)\equiv\begin{cases} 2 \pmod p & \text{if } p=x^2+xy+64y^2 \\ & \quad \text{or } p=3x^2+3xy+22y^2, \\ -1 \pmod p & \text{otherwise.} \end{cases}$$

(ii) *If $p\equiv 2 \pmod 3$, then*

$$U_{\frac{p+1}{3}}(9,-1)\equiv\begin{cases} 0 \pmod p & \text{if } p=8x^2+xy+8y^2 \\ & \quad \text{or } p=5x^2+5xy+14y^2, \\ \frac{14x+y}{17y} \pmod p & \text{if } p=35x^2+5xy+2y^2, \\ -\frac{22x+3y}{85y} \pmod p & \text{if } p=11x^2+3xy+6y^2\neq 11 \end{cases}$$

and

$$V_{\frac{p+1}{3}}(9,-1)\equiv\begin{cases} -2 \pmod p & \text{if } p=8x^2+xy+8y^2 \\ & \quad \text{or } p=5x^2+5xy+14y^2, \\ 1 \pmod p & \text{otherwise.} \end{cases}$$

Corollary 6.10. *Let $p>3$ be a prime such that $(\frac{-78}{p})=1$.*

(i) *If $p\equiv 1 \pmod 3$, then*

$$U_{\frac{p-1}{3}}(10,-1)\equiv\begin{cases} 0 \pmod p & \text{if } p=x^2+702y^2,\ 13x^2+54y^2, \\ -\frac{19x+y}{156y} \pmod p & \text{if } p=19x^2+2xy+37y^2\neq 19, \\ -\frac{79x+3y}{156y} \pmod p & \text{if } p=79x^2+6xy+9y^2\neq 79 \end{cases}$$

and

$$V_{\frac{p-1}{3}}(10,-1)\equiv\begin{cases} 2 \pmod p & \text{if } p=x^2+702y^2,\ 13x^2+54y^2, \\ -1 \pmod p & \text{otherwise.} \end{cases}$$

(ii) *If $p\equiv 2 \pmod 3$, then*

$$U_{\frac{p+1}{3}}(10,-1)\equiv\begin{cases} 0 \pmod p & \text{if } p=2x^2+351y^2,\ 26x^2+27y^2, \\ -\frac{29x+9y}{156y} \pmod p & \text{if } p=29x^2+18xy+27y^2\neq 29, \\ \frac{41x+6y}{156y} \pmod p & \text{if } p=41x^2+12xy+18y^2\neq 41 \end{cases}$$

and

$$V_{\frac{p+1}{3}}(10,-1)\equiv\begin{cases} -2 \pmod p & \text{if } p=2x^2+351y^2,\ 26x^2+27y^2, \\ 1 \pmod p & \text{otherwise.} \end{cases}$$

We note that the congruences for $U_{(p-(\frac{p}{3}))/3}(1,-1)$ and $U_{(p-(\frac{p}{3}))/3}(2,-1)$ $\pmod p$ have been given by the author in [S1].

Lemma 6.1. *Let $p>3$ be a prime and $P,Q\in\mathbb{Z}$ with $p\nmid PQ(P^2-4Q)$. Let $n=(p-(\frac{p}{3}))/6$.*

(i) *If $p\mid U_n(P,Q)$ or $p\mid U_{2n}(P,Q)$, then $\big(\frac{-3(P^2-4Q)}{p}\big)=1$.*

(ii) *Suppose $\big(\frac{-3(P^2-4Q)}{p}\big)=1$ and $P^2-4Q=df^2$ $(d,f\in\mathbb{Z})$. Then $p\mid U_{2n}(P,Q)$ if and only if $\big(\frac{P+f\sqrt{d}}{2}\big)^{2n}\equiv(\frac{Q}{p})Q^n \pmod p$.*

(iii) *$p\mid U_{2n}(P,Q)$ if and only if $V_{2n}(P,Q)\equiv 2(\frac{Q}{p})Q^n \pmod p$.*

(iv) *$p\mid U_n(P,Q)$ if and only if $(\frac{Q}{p})=1$ and $p\mid U_{2n}(P,Q)$.*

Proof. Let $U_m=U_m(P,Q)$ and $V_m=V_m(P,Q)$. For $k,m\in\mathbb{N}$ it is well known that $U_m\mid U_{km}$. Thus $U_n\mid U_{2n}$ and $U_{2n}\mid U_{p-(\frac{p}{3})}$. If $p\mid U_n$ or $p\mid U_{2n}$, we must have $p\mid U_{p-(\frac{p}{3})}$ and so $(\frac{-3(P^2-4Q)}{p})=1$ by [S1, Lemma 6.1]. This proves (i).

Now suppose $(\frac{-3(P^2-4Q)}{p})=1$ and $P^2-4Q=df^2$ with $d,f\in\mathbb{Z}$. From (6.1) we see that

$$p\mid U_{2n}\iff\Big(\frac{P-f\sqrt{d}}{P+f\sqrt{d}}\Big)^{2n}\equiv 1 \pmod p.$$

By the proof of Theorem 4.1, we have

$$\begin{aligned}\Big(\frac{P-f\sqrt{d}}{P+f\sqrt{d}}\Big)^{2n}&\equiv\Big(\frac{P^2-df^2}{p}\Big)(P^2-df^2)^{-n}(P+f\sqrt{d})^{2n}\\&=\Big(\frac{Q}{p}\Big)Q^{-n}\Big(\frac{P+f\sqrt{d}}{2}\Big)^{2n} \pmod p.\end{aligned}$$

Thus (ii) is true.

Now let us consider (iii). If $p\mid U_{2n}$, by (i) and (ii) we have $\big(\frac{-3(P^2-4Q)}{p}\big)=1$ and $\big(\frac{P\pm\sqrt{P^2-4Q}}{2}\big)^{2n}\equiv(\frac{Q}{p})Q^n \pmod p$. Thus $V_{2n}\equiv 2(\frac{Q}{p})Q^n \pmod p$ by (6.2). If $V_{2n}\equiv 2(\frac{Q}{p})Q^n \pmod p$, as $V_m^2-(P^2-4Q)U_m^2=4Q^m$ we see that $4Q^{2n}-(P^2-4Q)U_{2n}^2=4Q^{2n}$ and hence $p\mid U_{2n}$. So (iii) holds.

Finally we consider (iv). According to [S1, Lemma 6.1], $p\mid U_n$ if and only if $V_{2n}\equiv 2Q^n \pmod p$. On the other hand, $p\mid U_n$ implies $p\mid U_{2n}$ and so $V_{2n}\equiv 2(\frac{Q}{p})Q^n \pmod p$ by (iii). Hence $p\mid U_n$ implies $(\frac{Q}{p})=1$. Conversely, if $p\mid U_{2n}$ and $(\frac{Q}{p})=1$, by (iii) we have $V_{2n}\equiv 2(\frac{Q}{p})Q^n=2Q^n \pmod p$. Hence $p\mid U_n$. So (iv) holds and the proof is complete.

Suppose that $d>1$ is squarefree and $\varepsilon_d=(m+n\sqrt{d})/2$. Then the norm $N(\varepsilon_d)=(m^2-dn^2)/4=\pm1$. From Lemma 6.1(ii) we see that if p is a prime such that $p\equiv 1 \pmod 3$, $p\nmid mn$ and $(\frac{d}{p})=1$, then

$$\begin{aligned}\varepsilon_d\text{ is a cubic residue of }p&\iff\Big(\frac{m+n\sqrt{d}}{2}\Big)^{\frac{p-1}{3}}\equiv 1 \pmod p\\&\iff p\mid U_{\frac{p-1}{3}}(m,N(\varepsilon_d)).\end{aligned}\tag{6.3}$$

Theorem 6.2. *Let $p>3$ be a prime, and $P,Q\in\mathbb{Z}$ with $p\nmid PQ(P^2-4Q)$. Let $P^2-4Q=df^2$ $(d,f\in\mathbb{Z})$ and $k=k(P/(P,f),f/(P,f),d)$. Let*

$$M(P,Q,f)=\Big\{[a,b,c]\ \Big|\ [a,b,c]\in H(-3k^2d),\ (a,24Q/(P,f)^2)=1,\Big(\frac{\frac{bf}{(P,f)}-\frac{kP}{(P,f)}(1+2\omega)}{a}\Big)_3=1\Big\}.$$

(i) *$M(P,Q,f)$ is a subgroup of $H(-3k^2d)$. If $F(4Q/(P,f)^2)\nmid(2P/(P,f))$, then $|M(P,Q,f)|=h(-3k^2d)/3$.*

(ii) *$p\mid U_{(p-(\frac{p}{3}))/3}(P,Q)$ if and only if p is represented by a class in $M(P,Q,f)$.*

(iii) *$p\mid U_{(p-(\frac{p}{3}))/6}(P,Q)$ if and only if $(\frac{Q}{p})=1$ and p is represented by a class in $M(P,Q,f)$.*

Proof. Set $u=P/(P,f)$ and $v=f/(P,f)$. Then $(u,v)=1$, $u^2-dv^2=4Q/(P,f)^2$ and $k=k(u,v,d)$. It is easy to see that $M(P,Q,f)=G(u,v,d)$. Thus applying Corollary 3.2 we see that (i) holds. Using Lemma 6.1 and Theorem 6.1 (or Theorem 4.2) we deduce (ii) and (iii). So the theorem is proved.

Remark 6.2 In [S1], the author misunderstood Spearman-Williams' result in [SW1] since a subgroup of index 3 may be not the subgroup consisting of all cubes. Thus (5.5), Lemma 5.1, Theorem 5.4, Corollaries 5.3, 5.4 and 6.4 in [S1] are somewhat wrong. Now we have Theorem 6.2 instead of [S1, Corollary 6.4], and Corollary 4.2 instead of [S1, Corollary 5.4].

From Lemma 6.1 and Theorem 5.2 (or Theorem 6.2) we have:

Corollary 6.11. *Let $p>3$ be a prime, $m\in\mathbb{Z}$, $p\nmid m(m^2+4)$ and $m^2+4=dn^2$ $(d,n\in\mathbb{Z})$. Let k be as in Theorem 5.1. Then $p\mid U_{(p-(\frac{p}{3}))/3}(m,-1)$ if and only if p is represented by some class $[a,b,c]\in H(-3k^2d)$ with $(a,6)=1$ and $\big(\frac{bn-km(1+2\omega)}{a}\big)_3=1$.*

From Corollaries 6.3-6.6 or Theorem 6.2 we have:

Corollary 6.12. *Let $p>3$ be a prime.*

(i) *If $p\neq5$, then $p\mid U_{\frac{p-(\frac{p}{3})}{3}}(10,1)$ if and only if p is represented by x^2+162y^2 or $2x^2+81y^2$.*

(ii) *If $p\neq7$, then $p\mid U_{\frac{p-(\frac{p}{3})}{3}}(16,1)$ if and only if p is represented by x^2+189y^2, $7x^2+27y^2$, $2x^2+2xy+95y^2$ or $14x^2+14xy+17y^2$.*

(iii) *If $p\neq17$, then $p\mid U_{\frac{p-(\frac{p}{3})}{3}}(8,-1)$ if and only if p is represented by $x^2+xy+115y^2$ or $11x^2+5xy+11y^2$.*

(iv) *If $p\neq5,41$, then $p\mid U_{\frac{p-(\frac{p}{3})}{3}}(64,-1)$ if and only if p is represented by $x^2+xy+277y^2$ or $17x^2+7xy+17y^2$.*

Corollary 6.13. *Let $p \neq 2, 3, 13$ be a prime.*
(i) *If $p \equiv 1 \pmod 6$, then*

$$p \mid U_{\frac{p-1}{3}}(3,-1) \iff p = x^2 + 351y^2,\ 13x^2 + 27y^2,$$
$$p \mid U_{\frac{p-1}{6}}(3,-1) \iff p = x^2 + 1404y^2,\ 13x^2 + 108y^2.$$

Moreover, if $p \equiv 1 \pmod 6$ and $(\frac{p}{13}) = 1$, then $\varepsilon_{13} = (3+\sqrt{13})/2$ is a cubic residue of p if and only if p is represented by $x^2 + 351y^2$ or $13x^2 + 27y^2$.
(ii) *If $p \equiv 5 \pmod 6$, then*

$$p \mid U_{\frac{p+1}{3}}(3,-1) \iff p = 11x^2 + 2xy + 32y^2,$$
$$p \mid U_{\frac{p+1}{6}}(3,-1) \iff p = 41x^2 + 40xy + 44y^2.$$

Proof. By Lemma 6.1(i), we may assume $(\frac{p}{13}) = (\frac{p}{3})$. From Corollary 6.7 and Theorem 6.2 we see that if $p \equiv 1 \pmod 6$, then

$$p \mid U_{\frac{p-1}{3}}(3,-1) \iff p = x^2 + xy + 88y^2,\ 10x^2 + 7xy + 10y^2$$
$$p \mid U_{\frac{p-1}{6}}(3,-1) \iff p = 4k+1 = x^2 + xy + 88y^2,\ 10x^2 + 7xy + 10y^2;$$

if $p \equiv 5 \pmod 6$, then

$$p \mid U_{\frac{p+1}{3}}(3,-1) \iff p = 11x^2 + xy + 8y^2 \iff p = 11x^2 + 2xy + 32y^2,$$
$$p \mid U_{\frac{p+1}{6}}(3,-1) \iff p = 4k+1 = 11x^2 + 2xy + 32y^2.$$

For $p \equiv 1 \pmod 6$ we see that

$$\begin{aligned} p = x^2 + xy + 88y^2 &\iff p = x^2 + xy + 88y^2 \quad \text{with } 2 \mid y \\ &\iff p = x^2 + 2xy + 352y^2 = (x+y)^2 + 351y^2 \\ &\iff p = t^2 + 351y^2 \end{aligned}$$

and

$$\begin{aligned} & p = 10x^2 + 7xy + 10y^2 \\ &\iff p = 10x^2 + 7xy + 10y^2 \quad \text{with } 2 \nmid xy \\ &\iff p = 10\Big(\frac{x+y}{2} + \frac{x-y}{2}\Big)^2 + 7\Big(\frac{x+y}{2} + \frac{x-y}{2}\Big)\Big(\frac{x+y}{2} - \frac{x-y}{2}\Big) \\ &\qquad + 10\Big(\frac{x+y}{2} - \frac{x-y}{2}\Big)^2 \quad \text{with } 2 \nmid xy \\ &\iff p = 10(t+u)^2 + 7(t+u)(t-u) + 10(t-u)^2 \\ &\iff p = 13u^2 + 27t^2. \end{aligned}$$

Thus

$$\begin{aligned} p \mid U_{\frac{p-1}{6}}(3,-1) &\iff p = 4k+1 = x^2+xy+88y^2,\ 10x^2+7xy+10y^2 \\ &\iff p = 4k+1 = x^2+351y^2,\ 13x^2+27y^2 \\ &\iff p = x^2+351y^2,\ 13x^2+27y^2 \quad \text{with } 2 \mid y \\ &\iff p = x^2+1404y^2,\ 13x^2+108y^2. \end{aligned}$$

Now applying (6.3) we obtain (i).

For $p \equiv 5 \pmod 6$ we have

$$\begin{aligned} p \mid U_{\frac{p+1}{6}}(3,-1) &\iff p = 4k+1 = 11x^2+2xy+32y^2 \\ &\iff p = 11x^2+2xy+32y^2 \quad \text{with } 2 \mid x-y \\ &\iff p = 11(y+2t)^2+2(y+2t)y+32y^2 \\ &\iff p = 44t^2+48ty+45y^2. \end{aligned}$$

Observe that $(44,48,45) \sim (44,-40,41) \sim (41,40,44)$. We see that (ii) is true. The proof is now complete.

Using Theorem 6.2 and (6.3) one can similarly prove the following corollaries.

Corollary 6.14. *Let $p > 5$ be a prime.*

(i) *If $p \equiv 1 \pmod 6$, then*

$$\begin{aligned} p \mid U_{\frac{p-1}{3}}(6,-1) &\iff p = x^2+270y^2,\ 10x^2+27y^2, \\ p \mid U_{\frac{p-1}{6}}(6,-1) &\iff p = x^2+1080y^2,\ 37x^2+34xy+37y^2. \end{aligned}$$

Moreover, if $p \equiv 1 \pmod 6$ and $(\frac{10}{p}) = 1$, then $\varepsilon_{10} = 3+\sqrt{10}$ is a cubic residue of p if and only if p is represented by x^2+270y^2 or $10x^2+27y^2$.

(ii) *If $p \equiv 5 \pmod 6$, then*

$$\begin{aligned} p \mid U_{\frac{p+1}{3}}(6,-1) &\iff p = 2x^2+135y^2,\ 5x^2+54y^2, \\ p \mid U_{\frac{p+1}{6}}(6,-1) &\iff p = 8x^2+8xy+137y^2,\ 5x^2+216y^2. \end{aligned}$$

Corollary 6.15. *Let $p \neq 2,3,5,17$ be a prime.*

(i) *If $p \equiv 1 \pmod 6$, then*

$$\begin{aligned} p \mid U_{\frac{p-1}{3}}(9,-1) &\iff p = x^2+255y^2,\ 3x^2+85y^2, \\ p \mid U_{\frac{p-1}{6}}(9,-1) &\iff p = x^2+1020y^2,\ 12x^2+85y^2. \end{aligned}$$

Moreover, if $p \equiv 1 \pmod 6$ and $(\frac{p}{5}) = (\frac{p}{17})$, then $\varepsilon_{85} = (9+\sqrt{85})/2$ is a cubic residue of p if and only if p is represented by x^2+255y^2 or $3x^2+85y^2$.

(ii) *If $p \equiv 5 \pmod 6$, then*

$$\begin{aligned} p \mid U_{\frac{p+1}{3}}(9,-1) &\iff p = 5x^2+51y^2,\ 17x^2+15y^2, \\ p \mid U_{\frac{p+1}{6}}(9,-1) &\iff p = 5x^2+204y^2,\ 17x^2+60y^2. \end{aligned}$$

Corollary 6.16. *Let $p \neq 2, 3, 5, 13$ be a prime.*

(i) *If $p \equiv 1 \pmod 6$, then*

$$p \mid U_{\frac{p-1}{3}}(10, -1) \iff p = x^2 + 702y^2,\ 13x^2 + 54y^2,$$
$$p \mid U_{\frac{p-1}{6}}(10, -1) \iff p = x^2 + 2808y^2,\ 13x^2 + 216y^2.$$

Moreover, if $p \equiv 1 \pmod 6$ and $(\frac{26}{p}) = 1$, then $\varepsilon_{26} = 5 + \sqrt{26}$ is a cubic residue of p if and only if p is represented by $x^2 + 702y^2$ or $13x^2 + 54y^2$.

(ii) *If $p \equiv 5 \pmod 6$, then*

$$p \mid U_{\frac{p+1}{3}}(10, -1) \iff p = 2x^2 + 351y^2,\ 26x^2 + 27y^2,$$
$$p \mid U_{\frac{p+1}{6}}(10, -1) \iff p = 8x^2 + 8xy + 353y^2,\ 53x^2 + 2xy + 53y^2.$$

Theorem 6.3. *Suppose $m \in \mathbb{Z}$, $m^2 - 4 = dn^2$ $(d, n \in \mathbb{Z})$ and $\mathrm{ord}_3(m-2) \geq \mathrm{ord}_3 n$. Let $p > 3$ be a prime such that $p \nmid m^2 - 4$. Let k be as in Theorem 5.5. Suppose $p = ax^2 + bxy + cy^2$ with $a, b, c, x, y \in \mathbb{Z}$, $b^2 - 4ac = -3k^2 d$, $p \nmid a$ and $(a, 6(8-4m)/(m-2, n)^2) = 1$. Then*

$$U_{\frac{p-(\frac{p}{3})}{3}}(m, 1) \equiv \begin{cases} 0 \pmod p & \text{if } \left(\frac{\frac{bn}{(m-2,n)} + \frac{k(m-2)}{(m-2,n)}(1+2\omega)}{a}\right)_3 = 1, \\ -\left(\frac{p}{3}\right)\frac{2ax+by}{kdny} \pmod p & \text{if } \left(\frac{\frac{bn}{(m-2,n)} + \frac{k(m-2)}{(m-2,n)}(1+2\omega)}{a}\right)_3 = \omega, \\ \left(\frac{p}{3}\right)\frac{2ax+by}{kdny} \pmod p & \text{if } \left(\frac{\frac{bn}{(m-2,n)} + \frac{k(m-2)}{(m-2,n)}(1+2\omega)}{a}\right)_3 = \omega^2 \end{cases}$$

and

$$V_{\frac{p-(\frac{p}{3})}{3}}(m, 1) \equiv \begin{cases} 2 \pmod p & \text{if } \left(\frac{\frac{bn}{(m-2,n)} + \frac{k(m-2)}{(m-2,n)}(1+2\omega)}{a}\right)_3 = 1, \\ -1 \pmod p & \text{if } \left(\frac{\frac{bn}{(m-2,n)} + \frac{k(m-2)}{(m-2,n)}(1+2\omega)}{a}\right)_3 = \omega, \omega^2. \end{cases}$$

Proof. As $m^2 - 4 = dn^2$, from (6.1) and (6.2) we have

$$\begin{aligned} U_r(m, 1) &= \frac{1}{n\sqrt{d}}\left\{\left(\frac{m + n\sqrt{d}}{2}\right)^r - \left(\frac{m - n\sqrt{d}}{2}\right)^r\right\} \\ &= \frac{1}{n\sqrt{d}}\left\{\left(\frac{m + n\sqrt{d}}{2}\right)^r - \left(\frac{m + n\sqrt{d}}{2}\right)^{-r}\right\} \end{aligned}$$

and

$$V_r(m, 1) = \left(\frac{m + n\sqrt{d}}{2}\right)^r + \left(\frac{m - n\sqrt{d}}{2}\right)^r = \left(\frac{m + n\sqrt{d}}{2}\right)^r + \left(\frac{m + n\sqrt{d}}{2}\right)^{-r}.$$

Thus applying Theorem 5.5 we obtain the result.

From Lemma 6.1 and Theorem 5.6 we have:

Theorem 6.4. *Suppose* $m \in \mathbb{Z}$, $m^2-4 = dn^2$ $(d, n \in \mathbb{Z})$ *and* $\mathrm{ord}_3(m-2) \geq \mathrm{ord}_3 n$. *Let* $p > 3$ *be a prime such that* $p \nmid m^2-4$. *Let* k *be as in Theorem* 5.5. *Then* $p \mid U_{(p-(\frac{p}{3}))/3}(m, 1)$ *if and only if* p *is represented by a class in the subgroup* $L(m, n, d)$ *of* $H(-3k^2d)$, *where* $L(m, n, d)$ *is as in Theorem* 5.6.

7. Cubic congruences modulo a prime.

Let $p > 3$ be a prime and $a_1, a_2, a_3 \in \mathbb{Z}$. Let $N_p(x^3 + a_1x^2 + a_2x + a_3)$ denote the number of solutions of the congruence $x^3 + a_1x^2 + a_2x + a_3 \equiv 0 \pmod{p}$. Set

$$(7.1)\quad P = -2a_1^3 + 9a_1a_2 - 27a_3,\ Q = (a_1^2 - 3a_2)^3 \quad \text{and} \quad D = -\frac{P^2 - 4Q}{27}.$$

From [S2, Lemma 2.3] we know that D is the discriminant of $x^3 + a_1x^2 + a_2x + a_3$ and

$$(7.2)\quad N_p(x^3 + a_1x^2 + a_2x + a_3) = N_p(x^3 - 3Qx - PQ) \quad \text{when } p \nmid Q.$$

It is well known that (see [D], [Sk] and [S2])

$$(7.3)\qquad N_p(x^3 + a_1x^2 + a_2x + a_3) = \begin{cases} 0 \text{ or } 3 & \text{if } (\frac{D}{p}) = 1, \\ 3 & \text{if } (\frac{D}{p}) = 0, \\ 1 & \text{if } (\frac{D}{p}) = -1. \end{cases}$$

If $p \nmid Q$ and $p \mid P$, by (7.2) we see that $x^3 + a_1x^2 + a_2x + a_3 \equiv 0 \pmod{p}$ is solvable. Thus we need only to consider the congruence $x^3 - 3Qx - PQ \equiv 0 \pmod{p}$ under the condition $p \nmid PQ$ and $(\frac{-3(P^2-4Q)}{p}) = 1$.

Theorem 7.1. *Let* $p > 3$ *be a prime. Let* $P, Q \in \mathbb{Z}$, $p \nmid PQ(P^2 - 4Q)$, $P^2 - 4Q = df^2$ $(d, f \in \mathbb{Z})$ *and* $k = k(P/(P, f), f/(P, f), d)$. *Then the congruence* $x^3 - 3Qx - PQ \equiv 0 \pmod{p}$ *has three solutions if and only if* p *is represented by some class in* $M(P, Q, f)$, *where* $M(P, Q, f)$ *is a subgroup of* $H(-3k^2d)$ *given as in Theorem* 6.2.

Proof. Clearly the discriminant of $x^3 - 3Qx - PQ$ is $-27Q^2(P^2 - 4Q)$. Thus, by (7.3) we know that $N_p(x^3 - 3Qx - PQ) = 3$ implies $(\frac{-3(P^2-4Q)}{p}) = 1$. From Lemma 6.1(i) we also see that $p \mid U_{(p-(\frac{p}{3}))/3}(P, Q)$ implies $(\frac{-3(P^2-4Q)}{p}) = 1$. Thus, by [S1, Corollary 6.3] and (7.3) we have

$$(7.4)\qquad N_p(x^3 - 3Qx - PQ) = 3 \iff p \,\Big|\, U_{\frac{p-(\frac{p}{3})}{3}}(P, Q).$$

Now the result follows immediately from Theorem 6.2.

Putting $P = 2$, $d = 1 - Q$ and $f = 2$ in Theorem 7.1 and then applying (7.4) one can deduce the following result.

Corollary 7.1. *Let $p > 3$ be a prime, $Q \in \mathbb{Z}$ and $p \nmid Q(Q-1)$. Then the following statements are equivalent:*

(i) *The congruence $x^3 - 3Qx - 2Q \equiv 0 \pmod{p}$ has three solutions.*

(ii) $p \mid U_{(p-(\frac{p}{3}))/3}(2, Q)$.

(iii) *p is represented by some class $[a, b, c] \in H(3k^2(Q-1))$ with $(a, 6Q) = 1$ and $\left(\frac{b-k(1+2\omega)}{a}\right)_3 = 1$, where $k = k(1, 1, 1-Q)$.*

Putting $P = 6$, $d = 9 - Q$ and $f = 2$ in Theorem 7.1 and then applying (7.4) we deduce the following result.

Corollary 7.2. *Let $p > 3$ be a prime, $Q \in \mathbb{Z}$ and $p \nmid Q(Q-9)$. Then the following statements are equivalent:*

(i) *The congruence $x^3 - 3Qx - 6Q \equiv 0 \pmod{p}$ has three solutions.*

(ii) $p \mid U_{(p-(\frac{p}{3}))/3}(6, Q)$.

(iii) *p is represented by some class $[a, b, c] \in H(3k^2(Q-9))$ with $(a, 6Q) = 1$ and $\left(\frac{b-3k(1+2\omega)}{a}\right)_3 = 1$, where $k = k(3, 1, 9-Q)$.*

From (7.4) and Corollary 6.11 we have

Corollary 7.3. *Let $p > 3$ be a prime, $m \in \mathbb{Z}$, $p \nmid m(m^2+4)$ and $m^2 + 4 = dn^2$ $(d, n \in \mathbb{Z})$. Let k be as in Theorem 5.1. Then $x^3 + 3x + m \equiv 0 \pmod{p}$ has three solutions if and only if p is represented by some class $[a, b, c] \in H(-3k^2d)$ with $(a, 6) = 1$ and $\left(\frac{bn-km(1+2\omega)}{a}\right)_3 = 1$.*

From (7.4) and Corollaries 6.12-6.16 we have

Corollary 7.4. *Let $p > 3$ be a prime. Then*

(i) *If $p \neq 5$, then $N_p(x^3 - 3x - 10) = 3$ if and only if p is represented by $x^2 + 162y^2$ or $2x^2 + 81y^2$.*

(ii) *If $p \neq 7$, then $N_p(x^3 - 3x - 16) = 3$ if and only if p is represented by $x^2 + 189y^2$, $7x^2 + 27y^2$, $2x^2 + 2xy + 95y^2$ or $14x^2 + 14xy + 17y^2$.*

(iii) *If $p \neq 17$, then $N_p(x^3 + 3x + 8) = 3$ if and only if p is represented by $x^2 + xy + 115y^2$ or $11x^2 + 5xy + 11y^2$.*

(iv) *If $p \neq 5, 41$, then $N_p(x^3 + 3x + 64) = 3$ if and only if p is represented by $x^2 + xy + 277y^2$ or $17x^2 + 7xy + 17y^2$.*

(v) *If $p \neq 13$, then $N_p(x^3 + 3x + 3) = 3$ if and only if p is represented by $x^2 + 351y^2$, $13x^2 + 27y^2$ or $11x^2 + 2xy + 32y^2$.*

(vi) *If $p \neq 5$, then $N_p(x^3 + 3x + 6) = 3$ if and only if p is represented by $x^2 + 270y^2$, $10x^2 + 27y^2$, $2x^2 + 135y^2$ or $5x^2 + 54y^2$.*

(vii) *If $p \neq 5, 17$, then $N_p(x^3 + 3x + 9) = 3$ if and only if p is represented by $x^2 + 255y^2$, $3x^2 + 85y^2$, $5x^2 + 51y^2$ or $17x^2 + 15y^2$.*

(viii) *If $p \neq 5, 13$, then $N_p(x^3 + 3x + 10) = 3$ if and only if p is represented by $x^2 + 702y^2$, $13x^2 + 54y^2$, $2x^2 + 351y^2$ or $26x^2 + 27y^2$.*

Theorem 7.2. *Let $p > 3$ be a prime and $a_1, a_2, a_3 \in \mathbb{Z}$. Let P and Q be given by (7.1). Suppose $p \nmid PQ(P^2 - 4Q)$ and $P^2 - 4Q = df^2$ $(d, f \in \mathbb{Z})$. Then the congruence $x^3 + a_1x^2 + a_2x + a_3 \equiv 0 \pmod{p}$ has three solutions if*

and only if p is represented by some class in $M(P,Q,f)$, where $M(P,Q,f)$ is a subgroup of $H(-3k^2d)$ given as in Theorem 6.2.

Proof. This is immediate from (7.2) and Theorem 7.1.

Remark 7.1 Let us compare Theorem 7.2 with Theorem 1.4. First Spearman and Williams proved Theorem 1.4 using class field theory, and we prove Theorem 7.2 using the theory of cubic residues. Second, the subgroup $M(P,Q,f)$ in Theorem 7.2 is constructed, but Spearman and Williams only proved the existence of the subgroup $J(a_1,a_2,a_3)$. Third, in some special cases, the discriminant of corresponding quadratic forms in Theorem 1.4 seems better than the discriminant in Theorem 7.2.

References

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

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

[D] L.E. Dickson, *Criteria for the irreducibility of functions in a finite field*, Bull. Amer. Math. Soc. **13** (1906), 1-8.

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

[L1] E. Lehmer, *On Euler's criterion*, J. Austral. Math. Soc. **1** (1959/1961), part 1, 64-70.

[L2] E. Lehmer, *On the cubic character of quadratic units*, J. Number Theory **5** (1973), 385-389.

[Se] J.P. Serre, *On a theorem of Jordan*, Bull. Amer. Math. Soc. (New Series) **40** (2003), 429-440.

[Sk] T. Skolem, *On a certain connection between the discriminant of a polynomial and the number of its irreducible factors mod p*, Norsk Mat. Tidsskr. **34** (1952), 81-85.

[SW1] B.K. Spearman and K.S. Willimas, *The cubic congruence* $x^3+Ax^2+Bx+C\equiv 0 \pmod p$ *and binary quadratic forms*, Proc. London Math. Soc. **46** (1992), 397-410.

[SW2] B.K. Spearman and K.S. Willimas, *The cubic congruence* $x^3+Ax^2+Bx+C\equiv 0 \pmod p$ *and binary quadratic forms II*, J. London Math. Soc. **64** (2001), 273-274.

[S1] Z.H. Sun, *On the theory of cubic residues and nonresidues*, Acta Arith. **84** (1998), 291-335.

[S2] Z.H. Sun, *Cubic and quartic congruences modulo a prime*, J. Number Theory **102** (2003), 41-89.

[S3] Z.H. Sun, *Quartic residues and binary quadratic forms*, J. Number Theory **113** (2005), 10-52.

[S4] Z.H. Sun, *On the number of incongruent residues of* x^4+ax^2+bx *modulo p*, J. Number Theory **119** (2006), 210-241.

[W] P.J. Weinberger, *The cubic character of quadratic units*, Proc. 1972 Number Theory Conference, Univ. of Colorado, 1972, 241-242.

[Wi] K.S. Williams, *On Euler's criterion for cubic non-residues*, Proc. Amer. Math. Soc. **49** (1975), 277-283.