ACTA ARITHMETICA
LXXXIV.4 (1998)

On the theory of cubic residues and nonresidues

by

Zhi-Hong Sun (Huaiyin)

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 $N\pi = \pi\overline{\pi} = a^2-ab+b^2$. When $\pi \equiv 2 \pmod 3$ we say that π is *primary*.

If $\pi \in \mathbb{Z}[\omega],\ N\pi > 1$ and $\pi \equiv \pm 2 \pmod 3$ we may write $\pi = \pm\pi_1 \dots \pi_r$, where $\pi_1, \dots, \pi_r$ are primary primes. For $\alpha \in \mathbb{Z}[\omega]$ the *cubic Jacobi symbol* $\left(\frac{\alpha}{\pi}\right)_3$ is defined by

$$\left(\frac{\alpha}{\pi}\right)_3 = \left(\frac{\alpha}{\pi_1}\right)_3 \dots \left(\frac{\alpha}{\pi_r}\right)_3,$$

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

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

According to [IR, pp. 135, 313] 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 $\left(\frac{\omega}{a+b\omega}\right)_3 = \omega^{(a+b+1)/3}$.

(1.2) If $a,b \in \mathbb{Z}$ and $a+b\omega \equiv 2 \pmod 3$ then $\left(\frac{1-\omega}{a+b\omega}\right)_3 = \omega^{2(a+1)/3}$.

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

The assertion (1.3) is now called the *general cubic reciprocity law*; it was first proved by G. Eisenstein.

Let p be a prime of the form $3n+1$. It is well known that there are unique integers L and $|M|$ such that $4p = L^2+27M^2$ with $L \equiv 1 \pmod 3$. It follows that $\left(\frac{L}{3M}\right)^2 \equiv -3 \pmod p$ and therefore $m^{(p-1)/3} \equiv 1,\ \left(-1-\frac{L}{3M}\right)/2$ or $\left(-1+\frac{L}{3M}\right)/2 \pmod p$ for any integer $m \not\equiv 0 \pmod p$.

In 1827 Jacobi [J] established the following rational cubic reciprocity law.

1991 *Mathematics Subject Classification*: 11A15, 11E25.

THEOREM 1.1 (Jacobi). *Let q be a prime of the form $3n+1$, $q \neq p$ and $4q = L'^2 + 27M'^2$. Then q is a cubic residue modulo p if and only if $(LM' - L'M)/(LM' + L'M)$ is a cubic residue modulo q.*

In 1958, using the period equation of degree 3, E. Lehmer [L1] gave the following criterion for cubic residuacity.

THEOREM 1.2 (E. Lehmer). *If q is an odd prime different from p then q is a cubic residue of p if and only if either $LM \equiv 0 \pmod q$ or $L \equiv \mu M \pmod q$, where μ satisfies the congruence*

$$\mu^2 \equiv \frac{3u+1}{3u-3}\left(\frac{9}{2u+1}\right)^2 \pmod q$$

with $u \not\equiv 0, 1, -\frac{1}{2}, -\frac{1}{3} \pmod q$ and $\left(\frac{(3u+1)(3u-3)}{q}\right) = 1$. Here $\left(\frac{\cdot}{q}\right)$ is the Legendre symbol.

In 1975 K. S. Williams [W1] showed how to choose the sign of M so that $m^{(p-1)/3} \equiv \big(-1 - \frac{L}{3M}\big)/2 \pmod p$ when m is a cubic nonresidue modulo p.

Let ε_d be the fundamental unit in the quadratic field $\mathbb{Q}(\sqrt{d})$. In 1970's E. Lehmer [L3], [L4] began to study criteria for ε_d to be a cubic residue modulo p, where p is a prime of the form $3n+1$ satisfying $\left(\frac{d}{p}\right) = 1$.

Since the work of Euler, Gauss, Jacobi and Eisenstein (see [IR, p. 133]) it is known that cubic congruences are connected with binary quadratic forms. In 1992 B. K. Spearman and K. S. Williams [SW] showed that m is a cubic residue modulo p if and only if p can be represented by one of the third (composition) powers of primitive integral binary quadratic forms of discriminant $-27m^2$, where p is a prime greater than 3 for which $m \not\equiv 0 \pmod p$.

Let m be a positive integer, and $\mathbb{Z}_m$ the set of those rational numbers whose denominator is prime to m. Inspired by the above work of Jacobi, Lehmer and Williams we introduce the subsets $C_0(m), C_1(m)$ and $C_2(m)$ of $\mathbb{Z}_m$ for $m \not\equiv 0 \pmod 3$, where

$$C_i(m) = \left\{ k \,\middle|\, \left(\frac{k+1+2\omega}{m}\right)_3 = \omega^i,\ k \in \mathbb{Z}_m \right\} \quad \text{for } i = 0, 1, 2.$$

In Sections 2 and 3 we concentrate on the structure and properties of $C_0(m), C_1(m)$ and $C_2(m)$. Here are some typical results:

(1.4) Let p be a prime of the form $3n+1$ and hence $4p = L^2 + 27M^2$ for some $L, M \in \mathbb{Z}$ and $L \equiv 1 \pmod 3$. If q is a prime such that $M \not\equiv 0 \pmod q$ and $i \in \{0, 1, 2\}$ then $q^{(p-1)/3} \equiv \big(\big(-1 - \frac{L}{3M}\big)/2\big)^i \pmod p$ if and only if $L/(3M) \in C_i(q)$.

(1.5) Let p be a prime for which $p \equiv 1 \pmod 3$, $t^2 \equiv -3 \pmod p$ ($t \in \mathbb{Z}$), $k \in \mathbb{Z}_p$, $k^2+3 \not\equiv 0 \pmod p$ and $i \in \{0,1,2\}$. Then $k \in C_i(p)$ if and only if

$$\left(\frac{k-t}{k+t}\right)^{(p-1)/3} \equiv \left(\frac{-1-t}{2}\right)^i \pmod p.$$

(1.6) Let p be a prime greater than 3, $k \in \mathbb{Z}_p$ and $k^2+3 \not\equiv 0 \pmod p$. Then $k \in C_0(p)$ if and only if

$$k \equiv \frac{x^3-9x}{3x^2-3} \pmod p \qquad \text{for some integer } x.$$

If q is also a prime of the form $3n+1$ and $4q = L'^2+27M'^2$ ($L', M' \in \mathbb{Z}$) with $L' \equiv 1 \pmod 3$, in view of (1.4) and (1.5) we see that

$$q^{(p-1)/3} \equiv \left(\frac{-1-L/(3M)}{2}\right)^i \pmod p$$

if and only if

$$\left(\frac{LM'-L'M}{LM'+L'M}\right)^{(q-1)/3} \equiv \left(\frac{-1-L'/(3M')}{2}\right)^i \pmod q.$$

This generalizes Jacobi's result.

Combining (1.4) with (1.6) gives a simple criterion for cubic residuacity which improves Lehmer's result.

Section 4 is devoted to cubic congruences. Here are two main results:

(1.7) If $p > 3$ is a prime, $a, b \in \mathbb{Z}_p$, $p \nmid ab$ and $s^2 \equiv -3(b^2-4a) \pmod p$ for some $s \in \mathbb{Z}$, then the congruence $x^3 - 3ax - ab \equiv 0 \pmod p$ is solvable if and only if $s/b \in C_0(p)$.

(1.8) Suppose that p is a prime greater than 3 and that N is the number of values of x^3+Ax^2+Bx+C modulo p, where $A, B, C \in \mathbb{Z}$ and x runs over all integers. If $A^2 \not\equiv 3B \pmod p$ then $N = p - \big(p - \big(\frac{-3}{p}\big)\big)/3$. If $A^2 \equiv 3B \pmod p$ then $N = (p+2)/3$ or p according as $p \equiv 1 \pmod 3$ or $p \equiv 2 \pmod 3$.

In Section 5 the criteria for $s(d) \in C_i(p)$ ($i = 0, 1, 2$) are given in terms of binary quadratic forms, where $p > 3$ is a prime, $d \in \mathbb{Z}$, $p \nmid (d+3)$ and $(s(d))^2 \equiv d \pmod p$. In particular, sufficient and necessary conditions for $s(d) \in C_0(p)$ are described in the cases $d = -1, -2, -5, -6, -7$ and -15. As a consequence we obtain criteria for $\varepsilon_6, \varepsilon_{15}, \varepsilon_{21}$ to be cubic residues modulo p.

In Section 6 we mainly determine $u_{(p-(\frac{-3}{p}))/3}(a,b)$ modulo p, where $p > 3$ is a prime and $\{u_n(a,b)\}$ is the Lucas sequence given by $u_0(a,b) = 0$, $u_1(a,b) = 1$ and $u_{n+1}(a,b) = bu_n(a,b) - au_{n-1}(a,b)$ ($n \geq 1$). In particular, we obtain $F_{(p-(\frac{-3}{p}))/3} \pmod p$ and $P_{(p-(\frac{-3}{p}))/3} \pmod p$, where $\{F_n\}$ and $\{P_n\}$ denote the Fibonacci sequence and Pell sequence respectively.

To illustrate the connections in the above work I state the following result:

(1.9) Let p be a prime for which $\left(\frac{-3}{p}\right) = \left(\frac{5}{p}\right) = 1$, and q a prime of the form $3n+1$ satisfying $L^2 + 135M^2 \equiv 0 \pmod p$, where L and M are determined by $4q = L^2 + 27M^2$ $(L, M \in \mathbb{Z})$. Then the following statements are equivalent:

(a) p is a cubic residue modulo q.
(b) $s(-15) \in C_0(p)$.
(c) ε_5 $(= (1+\sqrt{5})/2)$ is a cubic residue modulo p.
(d) The congruence $x^3 + 3x + 1 \equiv 0 \pmod p$ is solvable.
(e) $p \mid F_{(p-1)/3}$.
(f) $p = x^2 + 135y^2$ for some integers x and y.

For later convenience we list the following notations:

$\omega = (-1+\sqrt{-3})/2$, $\mathbb{Z}$—the set of integers, $\mathbb{Z}^+$—the set of natural numbers, $\mathbb{Z}[\omega]$—the set $\{a + b\omega \mid a, b \in \mathbb{Z}\}$, $N\pi$—the norm of π, $\mathbb{Q}$—the set of rational numbers, $\mathbb{Z}_m$—the set of those rational numbers whose denominator is prime to m, $[x]$—the greatest integer not exceeding x, $[x]_p$—the set $\{k \mid k \equiv x \pmod p, k \in \mathbb{Z}_p\}$, (a,b)—the greatest common divisor of a and b, $[a,b]$—the least common multiple of a and b, $m \mid n$—m divides n, $m \nmid n$—m does not divide n, $\left(\frac{a}{p}\right)$—the Legendre symbol, $\left(\frac{\alpha}{\pi}\right)_3$—the cubic Jacobi symbol.

2. Basic properties of $C_i(m)$. Let $m \in \mathbb{Z}^+$ and $m \not\equiv 0 \pmod 3$. For $a, b \in \mathbb{Z}_m$ it is clear that there are unique integers $a_0, b_0 \in \{0, 1, \ldots, m-1\}$ satisfying $a \equiv a_0 \pmod m$ and $b \equiv b_0 \pmod m$. From this we may define

$$(a, m) = (a_0, m) \quad \text{and} \quad \left(\frac{a+b\omega}{m}\right)_3 = \left(\frac{a_0+b_0\omega}{m}\right)_3 \quad \text{for } m > 1.$$

When $m = 1$ define

$$(a, m) = 1 \quad \text{and} \quad \left(\frac{a+b\omega}{m}\right)_3 = 1.$$

One can easily verify the following facts:

(2.1) If $a, b, c, d \in \mathbb{Z}_m$ then

$$\left(\frac{a+b\omega}{m}\right)_3 \left(\frac{c+d\omega}{m}\right)_3 = \left(\frac{(a+b\omega)(c+d\omega)}{m}\right)_3.$$

(2.2) If $n \in \mathbb{Z}_m$ and $(m, n) = 1$ then $\left(\frac{n}{m}\right)_3 = 1$.

(2.3) If $a, b \in \mathbb{Z}_{m_1 m_2}$ then

$$\left(\frac{a+b\omega}{m_1 m_2}\right)_3 = \left(\frac{a+b\omega}{m_1}\right)_3 \left(\frac{a+b\omega}{m_2}\right)_3.$$

DEFINITION 2.1. Suppose $m \in \mathbb{Z}^+$ and $m \not\equiv 0 \pmod 3$. For $i = 0, 1, 2$ define

$$C_i(m) = \left\{ k \;\middle|\; \left(\frac{k+1+2\omega}{m}\right)_3 = \omega^i,\ k \in \mathbb{Z}_m \right\}.$$

From the above definition it is easy to prove the following results:

(2.4) $C_0(m) \cup C_1(m) \cup C_2(m) = \{k \mid (k^2+3, m) = 1,\ k \in \mathbb{Z}_m\}$.
(2.5) $k \in C_0(m)$ if and only if $-k \in C_0(m)$.
(2.6) $k \in C_1(m)$ if and only if $-k \in C_2(m)$.

EXAMPLE 2.1. Set $C_i^*(m) = C_i(m) \cap \{k \mid -m/2 < k \le m/2,\ k \in \mathbb{Z}\}$ for $i = 0, 1, 2$. Then

$$\begin{aligned}
C_0^*(5) &= \{0\}, & C_1^*(5) &= \{1, 2\};\\
C_0^*(7) &= \{0\}, & C_1^*(7) &= \{-1, 3\};\\
C_0^*(11) &= \{0, 5, -5\}, & C_1^*(11) &= \{-1, -2, 3, -4\};\\
C_0^*(13) &= \{0, 4, -4\}, & C_1^*(13) &= \{1, -2, -3, -5\};\\
C_0^*(17) &= \{0, 1, -1, 3, -3\}, & C_1^*(17) &= \{2, 4, -5, -6, 7, -8\};\\
C_0^*(19) &= \{0, 1, -1, 3, -3\}, & C_1^*(19) &= \{-2, 5, -6, 7, -8, -9\}.
\end{aligned}$$

PROPOSITION 2.1. *Suppose $m \in \mathbb{Z}^+$ and $m \not\equiv 0 \pmod 3$. Then $0 \in C_0(m)$.*

Proof. Since

$$\left(\frac{1+2\omega}{m}\right)_3 = \left(\frac{1+2\omega}{m}\right)_3^4 = \left(\frac{(1+2\omega)^4}{m}\right)_3 = \left(\frac{9}{m}\right)_3 = 1$$

we see that $0 \in C_0(m)$.

LEMMA 2.1. *Suppose that $m \in \mathbb{Z}^+, m \not\equiv 0 \pmod 3$, $k_1, k_2 \in \mathbb{Z}_m$, $((k_1^2+3)(k_2^2+3), m) = 1$, and m' is the greatest divisor of m for which $(m', k_1+k_2) = 1$. Then*

$$\left(\frac{k_1+1+2\omega}{m}\right)_3 \left(\frac{k_2+1+2\omega}{m}\right)_3 = \left(\frac{\frac{k_1k_2-3}{k_1+k_2}+1+2\omega}{m'}\right)_3.$$

Proof. Since $(k_1+1+2\omega)(k_2+1+2\omega) = k_1k_2 - 3 + (k_1+k_2)(1+2\omega)$ it is seen that

$$\begin{aligned}
&\left(\frac{k_1+1+2\omega}{m}\right)_3 \left(\frac{k_2+1+2\omega}{m}\right)_3\\
&\qquad = \left(\frac{k_1k_2-3+(k_1+k_2)(1+2\omega)}{m}\right)_3\\
&\qquad = \left(\frac{\frac{k_1k_2-3}{k_1+k_2}+1+2\omega}{m'}\right)_3 \left(\frac{k_1k_2-3+(k_1+k_2)(1+2\omega)}{m/m'}\right)_3.
\end{aligned}$$

When $m = m'$, we have

$$\left(\frac{k_1k_2 - 3 + (k_1 + k_2)(1 + 2\omega)}{m/m'}\right)_3 = 1.$$

Now assume that $m > m'$ and that p is a prime divisor of m/m'. It is clear that $k_1 + k_2 \equiv 0 \pmod p$ and therefore that

$$\left(\frac{k_1k_2 - 3 + (k_1 + k_2)(1 + 2\omega)}{p}\right)_3 = \left(\frac{k_1k_2 - 3}{p}\right)_3 = \left(\frac{-k_1^2 - 3}{p}\right)_3 = 1.$$

Thus,

$$\left(\frac{k_1k_2 - 3 + (k_1 + k_2)(1 + 2\omega)}{m/m'}\right)_3 = \prod_{p|m/m'} \left(\frac{k_1k_2 - 3 + (k_1 + k_2)(1 + 2\omega)}{p}\right)_3 = 1.$$

This completes the proof.

Proposition 2.2. *Let m be a positive integer not divisible by 3, and $i \in \{0, 1, 2\}$.*

(i) *If $k, k' \in \mathbb{Z}_m$ and $kk' \equiv -3 \pmod m$ then $k \in C_i(m)$ if and only if $k' \in C_i(m)$.*

(ii) *If $k_1, k_2 \in C_i(m)$ and $(k_1 + k_2, m) = 1$ then $(3 - k_1k_2)/(k_1 + k_2) \in C_i(m)$.*

Proof. Since $(k, m) = 1$, by Proposition 2.1 we have

$$\left(\frac{k' + 1 + 2\omega}{m}\right)_3 = \left(\frac{k}{m}\right)_3 \left(\frac{k' + 1 + 2\omega}{m}\right)_3 = \left(\frac{-3 + k + 2k\omega}{m}\right)_3 = \left(\frac{1 + 2\omega}{m}\right)_3 \left(\frac{k + 1 + 2\omega}{m}\right)_3 = \left(\frac{k + 1 + 2\omega}{m}\right)_3.$$

So (i) follows.

To prove (ii), we note that

$$\begin{aligned}\left(\frac{\frac{3-k_1k_2}{k_1+k_2} + 1 + 2\omega}{m}\right)_3 &= \left(\frac{\frac{k_1k_2-3}{k_1+k_2} - 1 - 2\omega}{m}\right)_3 \\ &= \overline{\left(\frac{\frac{k_1k_2-3}{k_1+k_2} + 1 + 2\omega}{m}\right)_3} = \overline{\left(\frac{\frac{k_1k_2-3}{k_1+k_2} + 1 + 2\omega}{m}\right)_3} \\ &= \overline{\left(\frac{k_1 + 1 + 2\omega}{m}\right)_3} \overline{\left(\frac{k_2 + 1 + 2\omega}{m}\right)_3} \\ &\qquad \text{(by Lemma 2.1)} \\ &= \overline{\omega^i} \cdot \overline{\omega^i} = \omega^i.\end{aligned}$$

PROPOSITION 2.3. *Let $m \in \mathbb{Z}^+$ with $m \not\equiv 0 \pmod 3$, and $k \in \mathbb{Z}_m$ with $((k^2-1)(k^2+3), m) = 1$. Then $(k^3-9k)/(3k^2-3) \in C_0(m)$.*

Proof. Clearly,

$$(k+1+2\omega)^3 = (k+1+2\omega)(k^2-3+2k(1+2\omega)) = k^3-9k+(3k^2-3)(1+2\omega).$$

Thus,

$$\left(\frac{\frac{k^3-9k}{3k^2-3}+1+2\omega}{m}\right)_3 = \left(\frac{k^3-9k+(3k^2-3)(1+2\omega)}{m}\right)_3 = \left(\frac{(k+1+2\omega)^3}{m}\right)_3 = 1.$$

The proof is now complete.

PROPOSITION 2.4. *Let $m_1, m_2 \in \mathbb{Z}^+$ be such that $m_1 m_2 \not\equiv 0 \pmod 3$, $k \in \mathbb{Z}$ and $i \in \{0,1,2\}$. If $m_1 \equiv m_2 \pmod{[9, k^2+3]}$ then $k \in C_i(m_1)$ if and only if $k \in C_i(m_2)$.*

Proof. Write $k+1+2\omega = (-1)^j \omega^s (1-\omega)^t \pi_1 \dots \pi_r$, where $\pi_1, \dots, \pi_r$ are primary primes in $\mathbb{Z}[\omega]$. Since $(k+1+2\omega)(k+1+2\omega^2) = k^2+3$ it is seen that $k^2+3 \equiv 0 \pmod{\pi_i}$ $(i = 1, \dots, r)$. Using Proposition 2.1 and (1.1) we find

$$\left(\frac{\omega(1-\omega)}{m_1}\right)_3 = \left(\frac{\omega(1-\omega)}{m_2}\right)_3 = 1 \quad \text{and} \quad \left(\frac{\omega}{m_1}\right)_3 = \left(\frac{\omega}{m_2}\right)_3.$$

Hence,

$$\left(\frac{k+1+2\omega}{m_1}\right)_3 = \left(\frac{(-1)^j \omega^{s-t}}{m_1}\right)_3 \left(\frac{\omega(1-\omega)}{m_1}\right)_3^t \prod_{i=1}^r \left(\frac{\pi_i}{m_1}\right)_3$$
$$= \left(\frac{\omega}{m_1}\right)_3^{s-t} \prod_{i=1}^r \left(\frac{m_1}{\pi_i}\right)_3 = \left(\frac{\omega}{m_2}\right)_3^{s-t} \prod_{i=1}^r \left(\frac{m_2}{\pi_i}\right)_3$$
$$= \left(\frac{k+1+2\omega}{m_2}\right)_3.$$

This proves the result.

Now we point out the connections between $C_i(m)$ $(i \in \{0,1,2\})$ and cubic residues.

THEOREM 2.1. *Let $p \equiv 1 \pmod 3$ be a prime, $4p = L^2+27M^2$ $(L, M \in \mathbb{Z})$ with $L \equiv 1 \pmod 3$, and $m = 2^\alpha 3^\beta m' m'' \in \mathbb{Z}^+$ with $m' = \max\{d \mid d \,|\, m, (d, 6M) = 1\}$ and $(6, m'') = 1$. Then, for $i = 0, 1, 2$,*

$$m^{(p-1)/3} \equiv \left(\frac{-1-L/(3M)}{2}\right)^i \pmod p$$

if and only if $L/(3M)\in C_{i'}(m')$, *where* $i'\in\{0,1,2\}$ *is determined by*

$$i'\equiv\begin{cases} i+\beta M \pmod 3 & \text{if } 3\mid\alpha \text{ or } 2\mid M,\\ i+\beta M+(-1)^{r+s} \pmod 3 & \\ \qquad\text{if } \alpha\equiv(-1)^r \pmod 3 \text{ and } L\equiv(-1)^{s-1}M \pmod 4.\end{cases}$$

Proof. Set $\pi=(L+3M)/2+3M\omega$. Then $\pi\in\mathbb{Z}[\omega]$. Clearly $\pi\equiv 2 \pmod 3$ and $N\pi=p$. Thus,

$$\begin{aligned} m^{(p-1)/3}&\equiv\left(\frac{-1-L/(3M)}{2}\right)^i \pmod p\\ &\Leftrightarrow m^{(p-1)/3}\equiv\left(\frac{-1-L/(3M)}{2}\right)^i\equiv\omega^i \pmod\pi\\ &\Leftrightarrow\left(\frac{2^\alpha m'm''}{\pi}\right)_3\left(\frac{\omega(1-\omega)}{\pi}\right)_3^{2\beta}=\left(\frac{m}{\pi}\right)_3=\omega^i\\ &\Leftrightarrow\left(\frac{\pi}{2^\alpha m'm''}\right)_3=\left(\frac{2^\alpha m'm''}{\pi}\right)_3=\omega^{i-2\beta M}=\omega^{i+\beta M}\\ &\qquad\qquad\text{(by (1.1), (1.2) and (1.3)).}\end{aligned}$$

Now let us calculate $\left(\frac{\pi}{m''}\right)_3$. Obviously $\left(\frac{\pi}{m''}\right)_3=1$ for $m''=1$. Assume that $m''>1$ and that q is a prime divisor of m''. It is clear that $q\mid M$ and so that $q\nmid L$. Thus,

$$\left(\frac{\pi}{m''}\right)_3=\prod_{q\mid m''}\left(\frac{(L+3M)/2+3M\omega}{q}\right)_3=\prod_{q\mid m''}\left(\frac{L/2}{q}\right)_3=1.$$

On the other hand,

$$\left(\frac{(L+3M)/2+3M\omega}{2}\right)_3=\begin{cases}\left(\dfrac{(L+3M)/2}{2}\right)_3 & \text{if } 2\mid M,\\ \left(\dfrac{3M\omega}{2}\right)_3=\left(\dfrac{\omega}{2}\right)_3=\omega & \\ \qquad\text{if } 2\nmid M \text{ and } L\equiv M \pmod 4,\\ \left(\dfrac{1+\omega}{2}\right)_3=\left(\dfrac{\omega}{2}\right)_3^2=\omega^{-1} & \\ \qquad\text{if } 2\nmid M \text{ and } L\equiv -M \pmod 4.\end{cases}$$

So

$$\left(\frac{\pi}{2^\alpha}\right)_3=\left(\frac{\pi}{2}\right)_3^\alpha=\begin{cases}1 & \text{if } 3\mid\alpha \text{ or } 2\mid M,\\ (\omega^{(-1)^{s-1}})^\alpha=\omega^{-(-1)^{s+r}} & \\ \qquad\text{if } 3\mid(\alpha-(-1)^r) \text{ and } 4\mid(L-(-1)^{s-1}M).\end{cases}$$

Putting the above together we see that

$$m^{(p-1)/3} \equiv \left(\frac{-1-L/(3M)}{2}\right)^i \pmod p \Leftrightarrow \left(\frac{\pi}{m'}\right)_3 = \omega^{i+\beta M}\left(\frac{\pi}{2^\alpha}\right)_3^{-1} = \omega^{i'}.$$

This concludes the proof.

COROLLARY 2.1. *Let p and q be distinct primes greater than 3, $p \equiv 1 \pmod 3$ and $4p = L^2 + 27M^2$ $(L, M \in \mathbb{Z})$ with $L \equiv 1 \pmod 3$. If $q \mid M$ then $q^{(p-1)/3} \equiv 1 \pmod p$. If $q \nmid M$ and $i \in \{0,1,2\}$ then*

$$q^{(p-1)/3} \equiv \left(\frac{-1-L/(3M)}{2}\right)^i \pmod p$$

if and only if $L/(3M) \in C_i(q)$.

REMARK 2.1. According to Theorem 2.1 the value of $m^{(p-1)/3} \pmod p$ can be completely determined. The special cases $m = 2, 3$ were treated by E. Lehmer [L2] and K. S. Williams [W1] respectively. When m is a prime for which $m \neq 2, 3, p$, it follows from Corollary 2.1 that $m^{(p-1)/3} \pmod p$ depends only on $L/(3M) \pmod m$. This important fact was first observed by Jacobi [J], and proved by E. Lehmer [L1] and K. S. Williams [W1].

LEMMA 2.2. *Let $p \neq 3$ be a prime and $k \in \mathbb{Z}_p$.*

(i) *If $p \equiv 1 \pmod 3$ and so $p = \lambda\overline{\lambda}$ with $\lambda \in \mathbb{Z}[\omega]$ and $\lambda \equiv 2 \pmod 3$ then*

$$\left(\frac{k+1+2\omega}{p}\right)_3 = \left(\frac{(k^2+3)(k-1-2\omega)}{\lambda}\right)_3.$$

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

$$\left(\frac{k+1+2\omega}{p}\right)_3 \equiv (k^2+3)^{(p-2)/3}(k+1+2\omega)^{(p+1)/3} \pmod p.$$

P r o o f. Suppose $p = \lambda\overline{\lambda} \equiv 1 \pmod 3$ with $\lambda \in \mathbb{Z}[\omega]$ and $\lambda \equiv 2 \pmod 3$. From the properties of the cubic residue character it is seen that

$$\begin{aligned}\left(\frac{k+1+2\omega}{p}\right)_3 &= \left(\frac{k+1+2\omega}{\lambda}\right)_3\left(\frac{k+1+2\omega}{\overline{\lambda}}\right)_3 \\ &= \left(\frac{k+1+2\omega}{\lambda}\right)_3\overline{\left(\frac{k-1-2\omega}{\lambda}\right)_3} \\ &= \left(\frac{k+1+2\omega}{\lambda}\right)_3\left(\frac{k-1-2\omega}{\lambda}\right)_3^2 \\ &= \left(\frac{(k^2+3)(k-1-2\omega)}{\lambda}\right)_3.\end{aligned}$$

For (ii), we note that

$$(k+1+2\omega)^p \equiv (k+1)^p + 2^p\omega^p \equiv k+1+2\omega^2 = k-1-2\omega \pmod p$$

and so

$$\begin{aligned}\left(\frac{k+1+2\omega}{p}\right)_3 &\equiv (k+1+2\omega)^{(p^2-1)/3} = (k+1+2\omega)^{\frac{p(p-2)}{3}+\frac{p-2}{3}+\frac{p+1}{3}}\\ &\equiv (k-1-2\omega)^{(p-2)/3}(k+1+2\omega)^{(p-2)/3}(k+1+2\omega)^{(p+1)/3}\\ &= (k^2+3)^{(p-2)/3}(k+1+2\omega)^{(p+1)/3} \pmod p.\end{aligned}$$

Now we are ready to give

THEOREM 2.2. *Let $p \neq 3$ be a prime, $i \in \{0,1,2\}$ and $k \in \mathbb{Z}_p$ with $k^2+3 \not\equiv 0 \pmod p$.*

(i) *If $p \equiv 1 \pmod 3$ and so $t^2 \equiv -3 \pmod p$ for some $t \in \mathbb{Z}_p$ then $k \in C_i(p)$ if and only if*

$$\left(\frac{k-t}{k+t}\right)^{(p-1)/3} \equiv \left(\frac{-1-t}{2}\right)^i \pmod p.$$

(ii) *If $p \equiv 2 \pmod 3$ then $k \in C_i(p)$ if and only if*

$$\left(\frac{k-1-2\omega}{k+1+2\omega}\right)^{(p+1)/3} \equiv \omega^i \pmod p.$$

Proof. Suppose $p \equiv 1 \pmod 3$, $4p = L^2+27M^2$ ($L, M \in \mathbb{Z}$) and $L \equiv 1 \pmod 3$. Since $(L/(3M))^2 \equiv t^2 \equiv -3 \pmod p$ we may choose M so that $L \equiv 3Mt \pmod p$. Set $\lambda = (L+3M)/2 + 3M\omega$. Then $\lambda \in \mathbb{Z}[\omega]$ and $\lambda \equiv 2 \pmod 3$. Clearly $N\lambda = p$ and

$$\omega \equiv \frac{-1-L/(3M)}{2} \pmod\lambda.$$

Thus, by Lemma 2.2 we have

$$\begin{aligned}\left(\frac{k+1+2\omega}{p}\right)_3 &= \left(\frac{(k^2+3)(k-1-2\omega)}{\lambda}\right)_3\\ &\equiv ((k^2+3)(k-1-2\omega))^{(p-1)/3}\\ &\equiv \left((k^2+3)\left(k+\frac{L}{3M}\right)\right)^{(p-1)/3}\\ &\equiv ((k+t)^2(k-t))^{(p-1)/3} \pmod\lambda.\end{aligned}$$

It then follows that

$$\begin{aligned}k \in C_i(p) &\Leftrightarrow \left(\frac{k+1+2\omega}{p}\right)_3 = \omega^i\\ &\Leftrightarrow ((k+t)^2(k-t))^{(p-1)/3} \equiv \left(\frac{-1-t}{2}\right)^i \pmod\lambda\end{aligned}$$

$$\Leftrightarrow ((k+t)^2(k-t))^{(p-1)/3} \equiv \left(\frac{-1-t}{2}\right)^i \pmod p$$

$$\Leftrightarrow \left(\frac{k-t}{k+t}\right)^{(p-1)/3} \equiv \left(\frac{-1-t}{2}\right)^i \pmod p.$$

This proves (i).

Now consider (ii). Note that $(k+1+2\omega)^p \equiv k-1-2\omega \pmod p$. Using Lemma 2.2 we see that

$$\begin{aligned}\left(\frac{k+1+2\omega}{p}\right)_3 &\equiv (k-1-2\omega)^{(p-2)/3}(k+1+2\omega)^{(p-2)/3}(k+1+2\omega)^{(p+1)/3}\\ &= \left(\frac{k-1-2\omega}{k+1+2\omega}\right)^{(p-2)/3}(k+1+2\omega)^{\frac{2(p-2)}{3}+\frac{p+1}{3}}\\ &= \left(\frac{k-1-2\omega}{k+1+2\omega}\right)^{(p+1)/3}\frac{k+1+2\omega}{k-1-2\omega}(k+1+2\omega)^{p-1}\\ &\equiv \left(\frac{k-1-2\omega}{k+1+2\omega}\right)^{(p+1)/3} \pmod p.\end{aligned}$$

This completes the proof.

From Theorem 2.2 we have the following rational cubic reciprocity law.

Corollary 2.2. *Let p and q be distinct primes, $p \equiv 1 \pmod 3$, $4p = L^2 + 27M^2$ $(L, M \in \mathbb{Z})$, $L \equiv 1 \pmod 3$, $q > 3$ and $i \in \{0,1,2\}$.*

(i) *If $q \equiv 1 \pmod 3$ and hence $4q = L'^2 + 27M'^2$ $(L', M' \in \mathbb{Z})$ then*

$$q^{(p-1)/3} \equiv \left(\frac{-1-L/(3M)}{2}\right)^i \pmod p$$

if and only if

$$\left(\frac{LM'-L'M}{LM'+L'M}\right)^{(q-1)/3} \equiv \left(\frac{-1-L'/(3M')}{2}\right)^i \pmod q.$$

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

$$q^{(p-1)/3} \equiv \left(\frac{-1-L/(3M)}{2}\right)^i \pmod p$$

if and only if

$$\left(\frac{L-3M-6M\omega}{L+3M+6M\omega}\right)^{(q+1)/3} \equiv \omega^i \pmod q.$$

Proof. If $q \mid M$, it follows from Corollary 2.1 that $q^{(p-1)/3} \equiv 1 \pmod p$. If $q \nmid M$, using Corollary 2.1 and Theorem 2.2 we see that

$$q^{(p-1)/3}\equiv\left(\frac{-1-L/(3M)}{2}\right)^i\pmod p\Leftrightarrow\frac{L}{3M}\in C_i(q)$$

$$\Leftrightarrow\begin{cases}\left(\dfrac{L/(3M)-L'/(3M')}{L/(3M)+L'/(3M')}\right)^{(q-1)/3}\equiv\left(\dfrac{-1-L'/(3M')}{2}\right)^i\pmod q\\ \qquad\qquad\qquad\qquad\qquad\qquad\text{if } q\equiv1\pmod3,\\ \left(\dfrac{L/(3M)-1-2\omega}{L/(3M)+1+2\omega}\right)^{(q+1)/3}\equiv\omega^i\pmod q\quad\text{if } q\equiv2\pmod3.\end{cases}$$

This completes the proof.

Remark 2.2. In the case $i=0$ Corollary 2.2(i) was first observed by Jacobi [J], and Corollary 2.2(ii) can be deduced from [W1]. Inspired by K. Burde's rational biquadratic reciprocity, H. von Lienen (see [Li], [Bu]) established the first rational cubic reciprocity law.

Theorem 2.3. *Let $p>3$ be a prime, $k\in\mathbb{Z}_p$ and $k^2+3\not\equiv0\pmod p$.*

(i) *If $p\equiv1\pmod3$ and so $t^2\equiv-3\pmod p$ for some $t\in\mathbb{Z}$ then $k\in C_0(p)$ if and only if $(k^2+3)(k+t)$ is a cubic residue (mod p).*

(ii) *If $p\equiv2\pmod3$ then $k\in C_0(p)$ if and only if*

$$\sum_{r\equiv(p+1)/3\pmod3}\binom{(p+1)/3}{r}\left(\frac{k+1}{2}\right)^r\equiv\frac13\left(\frac{k+3}{2}\right)^{(p+1)/3}+\frac13(2(k^2+3))^{-(p-2)/3}\pmod p.$$

Proof. If $p\equiv1\pmod3$, it follows from Theorem 2.2 that

$$\begin{aligned}k\in C_0(p)&\Leftrightarrow\left(\frac{k-t}{k+t}\right)^{(p-1)/3}\equiv1\pmod p\\&\Leftrightarrow((k^2+3)(k+t))^{(p-1)/3}\equiv1\pmod p\\&\Leftrightarrow(k^2+3)(k+t)\text{ is a cubic residue }(\mathrm{mod}\,p).\end{aligned}$$

This proves (i).

Now consider (ii). For $i=0,1,2$ set

$$A_i=\sum_{r\equiv i\pmod3}\binom{(p+1)/3}{r}\left(\frac{k+1}{2}\right)^{(p+1)/3-r}.$$

Then $A_0+A_1+A_2=(1+(k+1)/2)^{(p+1)/3}$ and hence

$$\left(\frac{k+1}{2}+\omega\right)^{(p+1)/3}=A_0+A_1\omega+A_2\omega^2=A_0-A_2+(A_1-A_2)\omega$$

$$= 2A_0 + A_1 - \left(\frac{k+3}{2}\right)^{(p+1)/3} + \left(A_0 + 2A_1 - \left(\frac{k+3}{2}\right)^{(p+1)/3}\right)\omega.$$

In view of Lemma 2.2(i) we obtain

$$2^{-(p+1)/3}(k^2+3)^{-(p-2)/3}\left(\frac{k+1+2\omega}{p}\right)_3$$
$$\equiv 2A_0 + A_1 - \left(\frac{k+3}{2}\right)^{(p+1)/3} + \left(A_0 + 2A_1 - \left(\frac{k+3}{2}\right)^{(p+1)/3}\right)\omega \pmod p.$$

If $\left(\frac{k+1+2\omega}{p}\right)_3 = 1$, it is clear that

$$\begin{cases} 2A_0 + A_1 \equiv \left(\frac{k+3}{2}\right)^{(p+1)/3} + 2^{-(p+1)/3}(k^2+3)^{-(p-2)/3} \pmod p, \\ A_0 + 2A_1 \equiv \left(\frac{k+3}{2}\right)^{(p+1)/3} \pmod p \end{cases}$$

and therefore that

$$3A_0 \equiv \left(\frac{k+3}{2}\right)^{(p+1)/3} + (2(k^2+3))^{-(p-2)/3} \pmod p.$$

If $\left(\frac{k+1+2\omega}{p}\right)_3 = \omega$, then we have

$$\begin{cases} 2A_0 + A_1 \equiv \left(\frac{k+3}{2}\right)^{(p+1)/3} \pmod p, \\ A_0 + 2A_1 \equiv \left(\frac{k+3}{2}\right)^{(p+1)/3} + 2^{-(p+1)/3}(k^2+3)^{-(p-2)/3} \pmod p \end{cases}$$

and hence

$$3A_0 \equiv \left(\frac{k+3}{2}\right)^{(p+1)/3} - \frac{1}{2}(2(k^2+3))^{-(p-2)/3} \pmod p. \tag{2.7}$$

If $\left(\frac{k+1+2\omega}{p}\right)_3 = \omega^2$, one can similarly prove that (2.7) holds.

Now, by the above, (ii) follows and the proof is complete.

Corollary 2.3. *Let m be the product of primes of the form $3n+1$, and hence $t^2 \equiv -3 \pmod m$ for some $t \in \mathbb{Z}$. If $x \in \mathbb{Z}$ and $(x(x^3-1), m) = 1$ then $\frac{x^3+1}{x^3-1}t \in C_0(m)$.*

P r o o f. Write $m = p_1 \ldots p_r$, where $p_1, \ldots, p_r$ are primes of the form $3n+1$. For $i = 1, \ldots, r$ it is clear that $t^2 \equiv -3 \pmod{p_i}$. Thus,

$$\left(\frac{x^3+1}{x^3-1}t\right)^2 + 3 \equiv 3\left(1 - \left(\frac{x^3+1}{x^3-1}\right)^2\right) \equiv -\frac{12x^3}{(x^3-1)^2} \not\equiv 0 \pmod{p_i}$$

and so

$$\left(\left(\frac{x^3+1}{x^3-1}t\right)^2 + 3\right)\left(\frac{x^3+1}{x^3-1}t + t\right) \equiv -\frac{12x^3}{(x^3-1)^2} \cdot \frac{2x^3 t}{x^3-1} \equiv \left(\frac{2x^2 t}{x^3-1}\right)^3 \pmod{p_i}.$$

Applying Theorem 2.3(i) we find $\frac{x^3+1}{x^3-1}t \in C_0(p_i)$ and hence

$$\left(\frac{\frac{x^3+1}{x^3-1}t + 1 + 2\omega}{m}\right)_3 = \prod_{i=1}^{r}\left(\frac{\frac{x^3+1}{x^3-1}t + 1 + 2\omega}{p_i}\right)_3 = 1.$$

This is the result.

3. The structure of $C_i'(p)$. In this section we introduce the sets $C_0'(p)$, $C_1'(p)$ and $C_2'(p)$, and study their group structure. As an application we confirm a conjecture due to K. S. Williams [W1].

Definition 3.1. Let $p \neq 3$ be a prime, $k \in \mathbb{Z}_p$, $[k]_p = \{x \mid x \equiv k \pmod{p},\ x \in \mathbb{Z}_p\}$ and $[\infty]_p = \{n/m \mid m, n \in \mathbb{Z},\ p \mid m,\ p \nmid n\}$. Define

$$C_0'(p) = \{[k]_p \mid k \in C_0(p)\} \cup \{[\infty]_p\},$$
$$C_1'(p) = \{[k]_p \mid k \in C_1(p)\} \quad \text{and} \quad C_2'(p) = \{[k]_p \mid k \in C_2(p)\}.$$

As an example, taking $p = 5$ we have $C_0'(5) = \{[0]_5, [\infty]_5\}$, $C_1'(5) = \{[1]_5, [2]_5\}$ and $C_2'(5) = \{[-1]_5, [-2]_5\}$.

Let p be a prime greater than 3,

$$D_p = \begin{cases} \mathbb{Z}/p\mathbb{Z} & \text{if } p \equiv 1 \pmod 3, \\ \mathbb{Z}[\omega]/p\mathbb{Z}[\omega] & \text{if } p \equiv 2 \pmod 3 \end{cases}$$

be the residue class ring modulo p, and U_p the multiplicative group of D_p. It is well known that U_p is a cyclic group of order $p^{(3-(\frac{-3}{p}))/2} - 1$. Denote the unique subgroup of order $p - \left(\frac{-3}{p}\right)$ of U_p by G_p. Then G_p is also a cyclic group. So

$$S_p = \begin{cases} \{g \mid g^{p-1} \equiv 1 \pmod p,\ g^n \not\equiv 1 \pmod p\ (n = 1, \ldots, p-2),\ g \in \mathbb{Z}\} \\ \qquad\qquad \text{if } p \equiv 1 \pmod 3, \\ \{g \mid g^{p+1} \equiv 1 \pmod p,\ g^n \not\equiv 1 \pmod p\ (n = 1, \ldots, p),\ g \in \mathbb{Z}[\omega]\} \\ \qquad\qquad \text{if } p \equiv 2 \pmod 3 \end{cases}$$
$$\neq \emptyset.$$

We are now ready to give

THEOREM 3.1. *Let p be a prime greater than 3 and $g \in S_p$. For $i = 0, 1, 2$ we have*

(i) $$|C_i'(p)| = \frac{p - \left(\frac{-3}{p}\right)}{3}.$$

(ii) $$C_i'(p) = \left\{ \left[\left(\frac{-3}{p}\right)(1 + 2g^{(p-(\frac{-3}{p}))/3}) \frac{g^{3r+i}+1}{g^{3r+i}-1} \right]_p \;\middle|\; r = 0, 1, \ldots, \left(p - \left(\frac{-3}{p}\right)\right)/3 - 1 \right\}.$$

P r o o f. Suppose $k \in \mathbb{Z}_p$ with $k^2 + 3 \not\equiv 0 \pmod p$. If $p \equiv 1 \pmod 3$, it is clear that $(-1 - 2g^{(p-1)/3})^2 \equiv -3 \pmod p$. For $i \in \{0, 1, 2\}$ it follows from Theorem 2.2 that

$$\begin{aligned} k \in C_i(p) &\Leftrightarrow \left(\frac{k + 1 + 2g^{(p-1)/3}}{k - 1 - 2g^{(p-1)/3}}\right)^{(p-1)/3} \equiv g^{i(p-1)/3} \pmod p \\ &\Leftrightarrow \frac{k + 1 + 2g^{(p-1)/3}}{k - 1 - 2g^{(p-1)/3}} \equiv g^{3r+i} \pmod p \\ &\qquad \text{for some } r \in \{0, 1, \ldots, (p-1)/3 - 1\} \\ &\Leftrightarrow k \equiv (1 + 2g^{(p-1)/3}) \frac{g^{3r+i}+1}{g^{3r+i}-1} \pmod p \\ &\qquad \text{for some } r \in \{0, 1, \ldots, (p-4)/3\}. \end{aligned}$$

If $p \equiv 2 \pmod 3$, it is clear that $g^{(p+1)/3} \equiv \omega$ or $\omega^2 \pmod p$. For $i \in \{0, 1, 2\}$ it follows from Theorem 2.2 that

$$\begin{aligned} k \in C_i(p) &\Leftrightarrow \left(\frac{k - 1 - 2g^{(p+1)/3}}{k + 1 + 2g^{(p+1)/3}}\right)^{(p+1)/3} \equiv g^{i(p+1)/3} \pmod p \\ &\Leftrightarrow \frac{k - 1 - 2g^{(p+1)/3}}{k + 1 + 2g^{(p+1)/3}} \equiv g^{3r+i} \pmod p \\ &\qquad \text{for some } r \in \{0, 1, \ldots, (p+1)/3 - 1\} \\ &\Leftrightarrow k \equiv -(1 + 2g^{(p+1)/3}) \frac{g^{3r+i}+1}{g^{3r+i}-1} \pmod p \\ &\qquad \text{for some } r \in \{0, 1, \ldots, (p-2)/3\}. \end{aligned}$$

To conclude the proof, we note that

$$\left[\left(\frac{-3}{p}\right)(1 + 2g^{(p-(\frac{-3}{p}))/3}) \frac{g^{3\cdot 0+0}+1}{g^{3\cdot 0+0}-1} \right]_p = [\infty]_p$$

and that

$$\frac{g^{3r_1+i}+1}{g^{3r_1+i}-1} = 1 + \frac{2}{g^{3r_1+i}-1} \not\equiv 1 + \frac{2}{g^{3r_2+i}-1} = \frac{g^{3r_2+i}+1}{g^{3r_2+i}-1} \pmod p$$

provided $r_1 \not\equiv r_2 \pmod{\left(p - \left(\frac{-3}{p}\right)\right)/3}$.

Corollary 3.1. *Let $p>3$ be a prime, and R_p a complete residue system modulo p. Then*

$$\sum_{k\in C_1(p)\cap R_p} k\equiv -\frac{1}{3}\pmod p.$$

Proof. Let $g\in S_p$ and $m=\big(p-\big(\frac{-3}{p}\big)\big)/3$. It follows from Theorem 3.1 that

$$\begin{aligned}\sum_{k\in C_1(p)\cap R_p} k&\equiv\left(\frac{-3}{p}\right)(1+2g^m)\sum_{r=0}^{m-1}\frac{g^{3r+1}+1}{g^{3r+1}-1}\\&=\left(\frac{-3}{p}\right)(1+2g^m)\left(m+\sum_{r=0}^{m-1}\frac{2}{g^{3r+1}-1}\right)\pmod p.\end{aligned}$$

Since

$$\begin{aligned}\sum_{r=0}^{m-1}\frac{1}{g^{3r+1}-1}&=\sum_{r=0}^{m-1}\frac{1}{(g^{3r+1})^m-1}\sum_{s=0}^{m-1}(g^{3r+1})^s\\&\equiv\sum_{r=0}^{m-1}\frac{1}{g^m-1}\sum_{s=0}^{m-1}g^s\cdot g^{3sr}=\frac{1}{g^m-1}\sum_{s=0}^{m-1}g^s\sum_{r=0}^{m-1}g^{3sr}\\&=\frac{1}{g^m-1}\left(m+\sum_{s=1}^{m-1}g^s\frac{1-g^{3sm}}{1-g^{3s}}\right)\equiv\frac{m}{g^m-1}\pmod p,\end{aligned}$$

we find

$$\begin{aligned}\sum_{k\in C_1(p)\cap R_p} k&\equiv\left(\frac{-3}{p}\right)(1+2g^m)\left(m+\frac{2m}{g^m-1}\right)\\&\equiv\left(\frac{-3}{p}\right)m(g^m-g^{2m})\frac{-g^{2m}}{g^m-1}\end{aligned}$$

(Note that $1+g^m+g^{2m}=(g^{3m}-1)/(g^m-1)\equiv 0\pmod p$.)

$$=\left(\frac{-3}{p}\right)mg^{3m}\equiv-\frac{1}{3}\pmod p.$$

We are done.

Remark 3.1. Corollary 3.1 is equivalent to a result conjectured by K. S. Williams [W1].

Corollary 3.2. *Let $p>3$ be a prime, and R_p a complete residue system modulo p. Then*

$$\begin{aligned}&\left|\left\{k\;\middle|\;k\in C_1(p)\cap R_p,\left(\frac{k^2+3}{p}\right)=1\right\}\right|\\&\quad=\left|\left\{k\;\middle|\;k\in C_1(p)\cap R_p,\left(\frac{k^2+3}{p}\right)=-1\right\}\right|=\frac{p-\big(\frac{-3}{p}\big)}{6}.\end{aligned}$$

P r o o f. Let $g \in S_p$. In view of Theorem 3.1 we can write

$$C_1(p) \cap R_p = \{k_r \,|\, r = 0, 1, \dots, (p - (\tfrac{-3}{p}))/3 - 1\},$$

where

$$k_r \equiv \left(\frac{-3}{p}\right)(1 + 2g^{(p-(\frac{-3}{p}))/3})\frac{g^{3r+1}+1}{g^{3r+1}-1} \pmod p.$$

From this it follows that

$$\begin{aligned} k_r^2 &\equiv (1 + 4g^{(p-(\frac{-3}{p}))/3} + 4g^{(2(p-(\frac{-3}{p})))/3})\left(1 + \frac{2}{g^{3r+1}-1}\right)^2 \\ &\equiv -3\left(1 + \frac{2}{g^{3r+1}-1}\left(2 + \frac{2}{g^{3r+1}-1}\right)\right) = -3 - \frac{3 \cdot 4 \cdot g^{3r+1}}{(g^{3r+1}-1)^2} \pmod p \end{aligned}$$

and so

$$\begin{aligned} \left(\frac{k_r^2+3}{p}\right) &\equiv (k_r^2+3)^{(p-1)/2} \equiv (-3 \cdot 4)^{(p-1)/2} \cdot g^{\frac{p-1}{2}(3r+1)} \cdot \frac{g^{3r+1}-1}{(g^{3r+1}-1)^p} \\ &\equiv \left(\frac{-3}{p}\right) g^{\frac{p-(\frac{-3}{p})}{2}(3r+1)} \cdot g^{\frac{(\frac{-3}{p})-1}{2}(3r+1)} \cdot \frac{g^{3r+1}-1}{g^{(3r+1)p}-1} \\ &\equiv \left(\frac{-3}{p}\right)(-1)^{3r+1} g^{\frac{(\frac{-3}{p})-1}{2}(3r+1)} \frac{g^{3r+1}-1}{g^{(\frac{-3}{p})(3r+1)}-1} \\ &= (-1)^{r+1} \pmod p. \end{aligned}$$

Thus,

$$\left(\frac{k_{2n}^2+3}{p}\right) = -\left(\frac{k_{2n+1}^2+3}{p}\right) = -1 \quad \text{for } n = 0, 1, \dots, (p - (\tfrac{-3}{p}))/6 - 1.$$

This proves the corollary.

THEOREM 3.2. *Let p be a prime greater than 3. For $[k]_p, [k']_p \in C_0'(p) \cup C_1'(p) \cup C_2'(p)$ define*

$$[k]_p * [k']_p = \left[\frac{kk'-3}{k+k'}\right]_p \qquad ([k]_p * [\infty]_p = [\infty]_p * [k]_p = [k]_p).$$

Then $C_0'(p) \cup C_1'(p) \cup C_2'(p)$ forms a cyclic group of order $p - (\frac{-3}{p})$, and $C_0'(p)$ is a subgroup of order $(p - (\frac{-3}{p}))/3$. Moreover, $C_0'(p)$, $C_1'(p)$ and $C_2'(p)$ are the three distinct cosets of $C_0'(p)$.

P r o o f. Suppose $g \in S_p$. From Theorem 3.1 we know that

$$C_0'(p) \cup C_1'(p) \cup C_2'(p) = \left\{[k_r]_p \,\middle|\, r = 0, 1, \dots, p - \left(\frac{-3}{p}\right) - 1\right\},$$

where

$$[k_r]_p = \left[\left(\frac{-3}{p}\right)(1 + 2g^{(p-(\frac{-3}{p}))/3})\frac{g^r+1}{g^r-1}\right]_p.$$

Since

$$\left[\frac{k_ik_j-3}{k_i+k_j}\right]_p=\left[\frac{\left(\left(\frac{-3}{p}\right)(1+2g^{(p-(\frac{-3}{p}))/3})\right)^2\cdot\frac{g^i+1}{g^i-1}\cdot\frac{g^j+1}{g^j-1}-3}{\left(\frac{-3}{p}\right)(1+2g^{(p-(\frac{-3}{p}))/3})\left(\frac{g^i+1}{g^i-1}+\frac{g^j+1}{g^j-1}\right)}\right]_p$$
$$=\left[\left(\frac{-3}{p}\right)(1+2g^{(p-(\frac{-3}{p}))/3})\frac{(g^i+1)(g^j+1)+(g^i-1)(g^j-1)}{(g^i+1)(g^j-1)+(g^i-1)(g^j+1)}\right]_p$$
$$=\left[\left(\frac{-3}{p}\right)(1+2g^{(p-(\frac{-3}{p}))/3})\frac{g^{i+j}+1}{g^{i+j}-1}\right]_p,$$

we see that

$$[k_i]_p*[k_j]_p=\left[\frac{k_ik_j-3}{k_i+k_j}\right]_p=[k_{\langle i+j\rangle}]_p,$$

where $\langle x\rangle$ denotes the least nonnegative residue of x modulo $p-\left(\frac{-3}{p}\right)$.

By the above, $C_0'(p)\cup C_1'(p)\cup C_2'(p)$ is a cyclic group generated by $[k_1]_p$. Applying Theorem 3.1 we see that $C_0'(p)$ is a cyclic group generated by $[k_3]_p$, and that $C_0'(p)$, $C_1'(p)$ and $C_2'(p)$ are the three cosets of $C_0'(p)$. The proof is now complete.

Corollary 3.3. *Let p be a prime greater than 3. Then*

$$C_0'(p)=\left\{\left[\frac{x^3-9x}{3x^2-3}\right]_p\,\middle|\,x\in\{0,1,\ldots,p-1\},\ x^2\not\equiv-3\pmod p\right\}.$$

Proof. Clearly

$$\left[\frac{1^3-9\cdot1}{3\cdot1^2-3}\right]_p=[\infty]_p\in C_0'(p).$$

Suppose $k\in\mathbb{Z}_p$. It follows from Theorem 3.2 that

$$\begin{aligned}[k]_p\in C_0'(p)&\Leftrightarrow[k]_p=[x]_p*[x]_p*[x]_p\\&\quad\text{for some }[x]_p\in C_0'(p)\cup C_1'(p)\cup C_2'(p)\\&\Leftrightarrow[k]_p=\left[\frac{x^2-3}{2x}\right]_p*[x]_p=\left[\frac{x^3-9x}{3x^2-3}\right]_p\text{ for some integer }x\\&\quad\text{satisfying }x^2+3\not\equiv0\pmod p\text{ and }x\in\{0,1,\ldots,p-1\}.\end{aligned}$$

So the result follows.

Corollary 3.4. *Let $p>3$ be a prime, $i\in\{0,1,2\}$ and $[k_i]_p\in C_i'(p)$. For $[k]_p\in C_0'(p)$ define*

$$\varphi([k]_p)=\left[\frac{kk_i-3}{k+k_i}\right]_p\qquad(\varphi([\infty]_p)=[k_i]_p).$$

Then φ is a one-to-one correspondence from $C_0'(p)$ to $C_i'(p)$.

P r o o f. In view of Theorem 3.2,

$$C_i'(p) = [k_i]_p C_0'(p) = \{\varphi([k]_p) \mid [k]_p \in C_0'(p)\}.$$

So the result follows.

REMARK 3.2. Corollaries 3.3 and 3.4 provide a simple method of calculating $C_0'(p)$, $C_1'(p)$ and $C_2'(p)$ for any prime $p > 3$.

4. Cubic congruences. Let p be a prime greater than 3. In this section we consider the general cubic congruence $x^3 + Ax^2 + Bx + C \equiv 0 \pmod p$, where $A, B, C \in \mathbb{Z}_p$.

In [St] Stickelberger showed that the number of solutions of $x^3 + Ax^2 + Bx + C \equiv 0 \pmod p$ is given by

$$N = \begin{cases} 0 \text{ or } 3 & \text{if } \left(\dfrac{D}{p}\right) = 1, \\ 1 & \text{if } \left(\dfrac{D}{p}\right) = -1, \end{cases}$$

where $D = A^2B^2 - 4B^3 - 4A^3C - 27C^2 + 18ABC$.

Since

$$x^3 + Ax^2 + Bx + C = \left(x + \frac{A}{3}\right)^3 - 3 \cdot \frac{A^2 - 3B}{9}\left(x + \frac{A}{3}\right) + \frac{2A^3 - 9AB + 27C}{27},$$

it is enough to discuss the congruence $x^3 - 3ax - ab \equiv 0 \pmod p$ $(a, b \in \mathbb{Z}_p)$.

LEMMA 4.1. *Assume that p is a prime greater than 3, $k \in \mathbb{Z}_p$ and $k^2 + 3 \not\equiv 0 \pmod p$. Then $k \in C_0(p)$ if and only if the congruence $x^3 - 9(k^2+3)x - 18(k^2+3) \equiv 0 \pmod p$ is solvable. Moreover, if $k \in C_0(p)$ then the solutions of the above congruence are given by*

$$x \equiv \begin{cases} (-3 + kt)u(1-u) \pmod p & \text{if } p \equiv 1 \pmod 3, \\ (k - 3 + 2k\omega)u(1-u) \pmod p & \text{if } p \equiv 2 \pmod 3, \end{cases}$$

where t and u satisfy $t^2 \equiv -3 \pmod p$ $(t \in \mathbb{Z})$ and

$$u^3 \equiv \begin{cases} \dfrac{k-t}{k+t} \pmod p \ (u \in \mathbb{Z}) & \text{if } p \equiv 1 \pmod 3, \\ \dfrac{k-1-2\omega}{k+1+2\omega} \pmod p \ (u \in \mathbb{Z}[\omega]) & \text{if } p \equiv 2 \pmod 3. \end{cases}$$

P r o o f. If $k \equiv 0 \pmod p$, then $k \in C_0(p)$. Clearly, the congruence $x^3 - 9(k^2+3)x - 18(k^2+3) \equiv 0 \pmod p$ has the solutions $x \equiv 6, -3, -3 \pmod p$. So the result is true when $p \mid k$.

Now assume $k \not\equiv 0 \pmod p$. It follows from Corollary 3.3 that

$$\begin{aligned} k \in C_0(p) &\Leftrightarrow k \equiv \frac{s^3 - 9s}{3s^2 - 3} \pmod p \text{ for some } s \in \{0, 1, \ldots, p-1\} \\ &\Leftrightarrow s^3 - 3ks^2 - 9s + 3k \equiv 0 \pmod p \text{ is solvable.} \end{aligned}$$

Set $x\equiv\frac{3(k-s)}{s}\pmod p$. Then

$$\begin{aligned}\frac{9k^2}{s^3}(s^3-3ks^2-9s+3k)&=9k^2-9k^2\cdot\frac{3k}{s}-9\left(\frac{3k}{s}\right)^2+\left(\frac{3k}{s}\right)^3\\&\equiv 9k^2-9k^2(x+3)-9(x+3)^2+(x+3)^3\\&=x^3-9(k^2+3)x-18(k^2+3)\pmod p.\end{aligned}$$

So $k\in C_0(p)$ if and only if $x^3-9(k^2+3)x-18(k^2+3)\equiv 0\pmod p$ is solvable.

Let $k\in C_0(p)$ and $r=t$ or $1+2\omega$ according as $p\equiv 1$ or $2\pmod 3$. From Theorem 2.2 we know that

$$\left(\frac{k-r}{k+r}\right)^{(p-(\frac{-3}{p}))/3}\equiv 1\pmod p.$$

So the congruence

$$u^3\equiv\frac{k-r}{k+r}\pmod p$$

is solvable. Suppose $u^3\equiv\frac{k-r}{k+r}\pmod p$ and $x\equiv(-3+kr)u(1-u)\pmod p$. Then

$$\begin{aligned}u^3(1-u)^3&=u^3(1-3u+3u^2-u^3)\\&\equiv\frac{k-r}{k+r}\left(\frac{2r}{k+r}-3u+3u^2\right)\pmod p\end{aligned}$$

and hence

$$\begin{aligned}x^3-9(k^2+3)x&\equiv(-3+kr)^3u^3(1-u)^3-9(k^2+3)(-3+kr)(u-u^2)\\&\equiv r^3(k+r)^3\frac{k-r}{k+r}\left(\frac{2r}{k+r}-3u+3u^2\right)\\&\quad-9r(k+r)^2(k-r)(u-u^2)\\&\equiv 18(k^2+3)\pmod p.\end{aligned}$$

When $p\equiv 2\pmod 3$ it is easily seen that $u^3\overline{u}^3\equiv 1\pmod p$ and so that $\overline{u}\equiv u^{-1}\pmod p$. Hence,

$$\begin{aligned}\overline{(k-3+2k\omega)u(1-u)}&=\overline{(1+2\omega)}\ \overline{(k+1+2\omega)}\ \overline{u}(1-\overline{u})\\&\equiv(-1-2\omega)(k-1-2\omega)\frac{1}{u}\left(1-\frac{1}{u}\right)\\&=(1+2\omega)(k-1-2\omega)\frac{u(1-u)}{u^3}\\&\equiv(k-3+2k\omega)u(1-u)\pmod p.\end{aligned}$$

This shows that $(k-3+2k\omega)u(1-u)$ is congruent to an integer modulo p.

By the above, the lemma is proved.

THEOREM 4.1. *Let $p>3$ be a prime, $a,b,s\in\mathbb{Z}_p$, $ab\not\equiv 0 \pmod p$ and $s^2\equiv -3(b^2-4a) \pmod p$. Then the congruence $x^3-3ax-ab\equiv 0 \pmod p$ is solvable if and only if $s/b\in C_0(p)$. Moreover, if $s/b\in C_0(p)$ then the solutions of the above congruence are given by*

$$x\equiv\begin{cases}\frac{1}{6}(st-3b)u(1-u) \pmod p & \text{if } p\equiv 1 \pmod 3,\\ \frac{1}{6}(s-3b+2s\omega)u(1-u) \pmod p & \text{if } p\equiv 2 \pmod 3,\end{cases}$$

where t and u satisfy $t^2\equiv -3 \pmod p$ $(t\in\mathbb{Z})$ and

$$u^3\equiv\begin{cases}\dfrac{s-bt}{s+bt} \pmod p \ (u\in\mathbb{Z}) & \text{if } p\equiv 1 \pmod 3,\\ \dfrac{s-b(1+2\omega)}{s+b(1+2\omega)} \pmod p \ (u\in\mathbb{Z}[\omega]) & \text{if } p\equiv 2 \pmod 3.\end{cases}$$

Proof. Set $k=s/b$. Then $k^2+3\equiv 12a/b^2\not\equiv 0 \pmod p$. It is clear that

$$\begin{aligned}x^3-9(k^2+3)x-18(k^2+3)&\equiv x^3-\frac{108a}{b^2}x-\frac{216a}{b^2}\\&=\left(\frac{6}{b}\right)^3\left(\left(\frac{b}{6}x\right)^3-3a\cdot\frac{b}{6}x-ab\right) \pmod p.\end{aligned}$$

So the result follows from Lemma 4.1.

COROLLARY 4.1. *Let $p>3$ be a prime and $a,b\in\mathbb{Z}_p$. Then the congruence $x^3-3ax-ab\equiv 0 \pmod p$ is unsolvable if and only if $-3(b^2-4a)\equiv k^2b^2 \pmod p$ for some $k\in C_1(p)$.*

Proof. If $ab\equiv 0 \pmod p$ then $0^3-3a\cdot 0-ab\equiv 0 \pmod p$. If $b^2-4a\equiv 0 \pmod p$ then $b^3-3ab-ab\equiv 0 \pmod p$. So $x^3-3ax-ab\equiv 0 \pmod p$ is solvable when $ab(b^2-4a)\equiv 0 \pmod p$.

Now assume $ab(b^2-4a)\not\equiv 0 \pmod p$. Since $-4(-3a)^3-27(-ab)^2=-3(b^2-4a)\cdot 9a^2$, using Stickelberger's result we see that $x^3-3ax-ab\equiv 0 \pmod p$ has one solution if $\left(\frac{-3(b^2-4a)}{p}\right)=-1$.

If $\left(\frac{-3(b^2-4a)}{p}\right)=1$, there is an integer k such that $k^2\equiv -3(b^2-4a)/b^2 \pmod p$. Since $k^2+3\equiv 12a/b^2\not\equiv 0 \pmod p$ we have $k\in C_0(p)\cup C_1(p)\cup C_2(p)$. Applying Theorem 4.1 we see that $x^3-3ax-ab\equiv 0 \pmod p$ is solvable if and only if $k\in C_0(p)$. So $x^3-3ax-ab\equiv 0 \pmod p$ is unsolvable if and only if $-3(b^2-4a)\equiv k^2b^2 \pmod p$ for some $k\in C_1(p)\cup C_2(p)$.

Since $k\in C_2(p)$ if and only if $-k\in C_1(p)$, by the above the corollary is proved.

REMARK 4.1. If p is a prime greater than 3, $a,b\in\mathbb{Z}_p$ and $\left(\frac{-3(b^2-4a)}{p}\right)=-1$, one can easily check that the unique solution of $x^3-3ax-ab\equiv 0 \pmod p$ is given by

$$x\equiv a^{(p-(\frac{-3}{p}))/3}v_{(p+2(\frac{-3}{p}))/3}\pmod p,$$

where $\{v_n\}$ is defined by $v_0=2, v_1=b$ and $v_{n+1}=bv_n-av_{n-1}$ $(n\ge 1)$.

As applications of Theorem 4.1 we have

THEOREM 4.2. *Let $p>3$ be a prime, $m,n\in\mathbb{Z}_p$ and $mn\not\equiv 0\pmod p$. Then*

$$\left|\left\{\left[\frac{x^3}{mx+n}\right]_p\ \middle|\ x\not\equiv -\frac{n}{m}\pmod p,\ x\in\mathbb{Z}_p\right\}\right|=p-\frac{p-\left(\frac{-3}{p}\right)}{3}.$$

Proof. Set $b=3n/m$. Then $b\in\mathbb{Z}_p$ and $b\not\equiv 0\pmod p$. From Corollary 4.1 and Theorem 3.1(i) we see that

$$\begin{aligned}&\left|\left\{\left[\frac{x^3}{mx+n}\right]_p\ \middle|\ x\in\mathbb{Z}_p,\ x\not\equiv -\frac{n}{m}\pmod p\right\}\right|\\&\quad=\left|\left\{\left[\frac{x^3}{3x+b}\right]_p\ \middle|\ x\in\mathbb{Z}_p,\ x\not\equiv -\frac{b}{3}\pmod p\right\}\right|\\&\quad=|\{[a]_p\mid x^3-3ax-ab\equiv 0\pmod p\text{ is solvable}\}|\\&\quad=p-|\{[a]_p\mid x^3-3ax-ab\equiv 0\pmod p\text{ is unsolvable}\}|\\&\quad=p-|\{[a]_p\mid -3(b^2-4a)\equiv k^2b^2\pmod p\text{ for some }k\in C_1(p)\}|\\&\quad=p-\left|\left\{\left[\frac{(k^2+3)b^2}{12}\right]_p\ \middle|\ k\in C_1(p)\right\}\right|=p-\frac{p-\left(\frac{-3}{p}\right)}{3}.\end{aligned}$$

We are done.

THEOREM 4.3. *Let $p>3$ be a prime and $A,B,C\in\mathbb{Z}_p$. Then*

$$\begin{aligned}&|\{[x^3+Ax^2+Bx+C]_p\mid x\in\mathbb{Z}_p\}|\\&\quad=|\{[x^3+Ax^2+Bx+C]_p\mid x\in\{0,1,\ldots,p-1\}\}|\\&\quad=\begin{cases}\dfrac{p+2}{3} & \text{if } p\equiv 1\pmod 3 \text{ and } A^2\equiv 3B\pmod p,\\ p & \text{if } p\equiv 2\pmod 3 \text{ and } A^2\equiv 3B\pmod p,\\ p-\dfrac{p-\left(\frac{-3}{p}\right)}{3} & \text{if } A^2\not\equiv 3B\pmod p.\end{cases}\end{aligned}$$

Proof. Since

$$x^3+Ax^2+Bx+C=\left(x+\frac{A}{3}\right)^3-\frac{A^2-3B}{3}\left(x+\frac{A}{3}\right)+\frac{2A^3-9AB+27C}{27}$$

we see that

$$
\begin{aligned}
&|\{[x^3+Ax^2+Bx+C]_p \mid x\in\mathbb{Z}_p\}|\\
&\quad=\left|\left\{\left[x^3-\frac{A^2-3B}{3}x+\frac{2A^3-9AB+27C}{27}\right]_p \,\middle|\, x\in\mathbb{Z}_p\right\}\right|\\
&\quad=\left|\left\{\left[x^3-\frac{A^2-3B}{3}x\right]_p \,\middle|\, x\in\mathbb{Z}_p\right\}\right|\\
&\quad=\left|\left\{[t]_p \,\middle|\, x^3-\frac{A^2-3B}{3}x\equiv t \pmod p \text{ is solvable},\ t\in\mathbb{Z}_p\right\}\right|\\
&\quad=\begin{cases}
1+\dfrac{p-1}{3} & \text{if } p\equiv 1 \pmod 3 \text{ and } A^2\equiv 3B \pmod p,\\[2ex]
p & \text{if } p\equiv 2 \pmod 3 \text{ and } A^2\equiv 3B \pmod p,\\[2ex]
\left|\left\{[b]_p \,\middle|\, x^3-3\cdot\dfrac{A^2-3B}{9}x-\dfrac{A^2-3B}{9}b\equiv 0 \pmod p \text{ is solvable}\right\}\right| & \\[2ex]
\qquad\text{if } A^2\not\equiv 3B \pmod p.
\end{cases}
\end{aligned}
$$

Now suppose $A^2\not\equiv 3B \pmod p$ and $a=(A^2-3B)/9$. By Corollaries 4.1 and 3.2 we get

$$
\begin{aligned}
&|\{[b]_p \mid x^3-3ax-ab\equiv 0 \pmod p \text{ is solvable}\}|\\
&\quad=p-|\{[b]_p \mid x^3-3ax-ab\equiv 0 \pmod p \text{ is unsolvable}\}|\\
&\quad=p-|\{[b]_p \mid -3(b^2-4a)\equiv k^2b^2 \pmod p \text{ for some } k\in C_1(p)\}|\\
&\quad=p-\left|\left\{[b]_p \,\middle|\, b^2\equiv\frac{12a}{k^2+3} \pmod p \text{ for some } k\in C_1(p)\right\}\right|\\
&\quad=p-2\left|\left\{\left[\frac{12a}{k^2+3}\right]_p \,\middle|\, \left(\frac{k^2+3}{p}\right)=\left(\frac{12a}{p}\right),\ k\in C_1(p)\right\}\right|\\
&\quad=p-2\cdot\frac{p-\left(\frac{-3}{p}\right)}{6}.
\end{aligned}
$$

Putting the above together yields the result.

5. Connections with binary quadratic forms. Let d be a squarefree integer, and p a prime greater than 3 satisfying $\left(\frac{d}{p}\right)=1$. In this section we obtain a criterion for $s(d)\in C_i(p)$ $(i\in\{0,1,2\})$ in terms of the binary quadratic forms of discriminant $4d$, where $s(d)$ satisfies $(s(d))^2\equiv d \pmod p$.

THEOREM 5.1. *Let p be a prime greater than 3 and $p=ax^2+2bxy+cy^2$ with $a,b,c,x,y\in\mathbb{Z}$. If $d=b^2-ac$, $a=2^\alpha 3^r a_1$ $(2\nmid a_1, 3\nmid a_1)$, $d+3=2^\beta 3^s d_1$ $(2\nmid d_1, 3\nmid d_1)$, $(a,d+3)=1$ and $a(d+3)\not\equiv 0 \pmod p$, then*

$$\left(\frac{ax+(b+1)y+2y\omega}{a_1d_1^2p}\right)_3$$
$$=\begin{cases}\omega^{(1-s)(\frac{-3}{ax})\frac{y}{3}} & \text{if } y\equiv 0 \pmod 3,\\ \omega^{f_1(u)} & \text{if } a\equiv 0 \pmod 3 \text{ and } x\equiv uy \pmod 9,\\ \omega^{f_2(u)} & \text{if } a(ax+by)\not\equiv 0 \pmod 3 \text{ and } x\equiv uy \pmod 9,\\ 1 & \text{if } ax+by\equiv 0 \pmod 9,\\ \omega^{\pm(\frac{-3}{d})} & \text{if } ax+by\equiv \pm 3y \pmod 9,\end{cases}$$

where

$$f_1(u)=\frac{1}{3}\left(\frac{-3}{b}\right)\left((2bu+c)\left(\frac{-3}{2bu+c}\right)-1\right.$$
$$\left.+(r-1)\left(1-b\left(\frac{-3}{b}\right)\right)+ac+2^\alpha a_1\left(\frac{-3}{2^\alpha a_1}\right)-4\right),$$
$$f_2(u)=\frac{1}{3}\left(\frac{-3}{au+b}\right)\left(\left(s-\left(\frac{-3}{1-d}\right)\right)\left((au+b)\left(\frac{-3}{au+b}\right)-1\right)\right.$$
$$\left.+(1-d)\left(\frac{-3}{1-d}\right)-2^\beta d_1\left(\frac{-3}{2^\beta d_1}\right)\right)$$

and

$$\left(\frac{-3}{m}\right)=\begin{cases}1 & \text{if } m\equiv 1 \pmod 3,\\ -1 & \text{if } m\equiv -1 \pmod 3.\end{cases}$$

P r o o f. For later use we first point out the following facts:

(i) $y\not\equiv 0 \pmod p$. Indeed, if $p\,|\,y$ then $p\,|\,ax^2$ and so $p\mid x$. Thus, $p=ax^2+2bxy+cy^2\equiv 0 \pmod{p^2}$. This is a contradiction.

(ii) If $\pi=ax+by+y+2y\omega$ then $(N\pi,a)=(N\pi,d+3)=1$. Indeed, clearly $N\pi=\pi\overline{\pi}=(ax+by)^2+3y^2=ap+(d+3)y^2$. Thus, $(N\pi,a)=((d+3)y^2,a)=1$ and $(N\pi,d+3)=(ap,d+3)=1$.

(iii) If $A+B\omega\in\mathbb{Z}[\omega]$ and $A+B\omega\equiv 2 \pmod 3$ then $\left(\frac{3}{A+B\omega}\right)_3=\omega^{-B/3}$. Indeed, since $3=-\omega^2(1-\omega)^2$, it follows from (1.1) and (1.2) that

$$\left(\frac{3}{A+B\omega}\right)_3=\left(\frac{\omega}{A+B\omega}\right)_3^2\left(\frac{1-\omega}{A+B\omega}\right)_3^2$$
$$=\omega^{2(A+B+1)/3}\cdot\omega^{4(A+1)/3}=\omega^{-B/3}.$$

Now let $\pi=ax+(b+1)y+2y\omega$. Since $N(1-\omega)=3$ and $N\pi=(ax+by)^2+3y^2\not\equiv 0 \pmod 9$, there are integers $i,k\in\{0,1\}$ and $j\in\{0,1,2\}$ such that $\pi=(-1)^i\omega^j(1-\omega)^k\pi'$, where $\pi'\in\mathbb{Z}[\omega]$ and $\pi'\equiv 2 \pmod 3$.

Assume $y=3^t y_0$ $(3\nmid y_0)$ and $\pi'=A+B\omega$. Then we have

$$\begin{aligned}
\left(\frac{ax+(b+1)y+2y\omega}{p}\right)_3 &= \left(\frac{(-1)^i\omega^j(1-\omega)^k\pi'}{p}\right)_3\\
&= \left(\frac{\omega}{p}\right)_3^{j-k}\left(\frac{\omega(1-\omega)}{p}\right)_3^{k}\left(\frac{\pi'}{p}\right)_3 = \left(\frac{\omega}{p}\right)_3^{j-k}\left(\frac{1+2\omega}{p}\right)_3^{k}\left(\frac{p}{\pi'}\right)_3\\
&= \left(\frac{\omega}{p}\right)_3^{j-k}\left(\frac{ap}{\pi'}\right)_3\left(\frac{a^2}{\pi'}\right)_3 = \left(\frac{\omega}{p}\right)_3^{j-k}\left(\frac{-(d+3)y^2}{\pi'}\right)_3\left(\frac{a^2}{\pi'}\right)_3\\
&= \left(\frac{\omega}{p}\right)_3^{j-k}\left(\frac{3^{2r+s+2t}}{\pi'}\right)_3\left(\frac{2^{2\alpha+\beta}a_1^2d_1y_0^2}{\pi'}\right)_3\\
&= \left(\frac{\omega}{p}\right)_3^{j-k}\left(\frac{3}{\pi'}\right)_3^{s-r-t}\left(\frac{\pi'}{2^{2\alpha+\beta}a_1^2d_1y_0^2}\right)_3\\
&= \left(\frac{\omega}{p}\right)_3^{j-k}\omega^{-(s-r-t)B/3}\left(\frac{\pi}{2^{2\alpha+\beta}a_1^2d_1y_0^2}\right)_3\left(\frac{(-1)^i\omega^{j-k}(1+2\omega)^k}{2^{2\alpha+\beta}a_1^2d_1y_0^2}\right)_3^{-1}\\
&= \left(\frac{\omega}{p}\right)_3^{j-k}\omega^{(r+t-s)B/3}\left(\frac{\omega}{2^{2\alpha+\beta}a_1^2d_1y_0^2}\right)_3^{k-j}\left(\frac{\pi}{a_1^2d_1}\right)_3\left(\frac{\pi}{2}\right)_3^{2\alpha+\beta}\left(\frac{\pi}{y_0}\right)_3^{2}\\
&\qquad\qquad\text{(by Proposition 2.1)}\\
&= \left(\frac{\omega}{p}\right)_3^{j-k}\omega^{(r+t-s)B/3}\left(\frac{\omega}{2^{2\alpha+\beta}a_1^2d_1y_0^2}\right)_3^{2(j-k)}\left(\frac{\pi}{a_1^2d_1}\right)_3\\
&\qquad\qquad\text{(Note that } \left(\tfrac{\pi}{2}\right)_3=\left(\tfrac{\pi}{y_0}\right)_3=1.\text{)}\\
&= \left(\frac{\omega}{2^{\alpha+2\beta}a_1d_1^2py_0}\right)_3^{j-k}\omega^{(r+t-s)B/3}\left(\frac{\pi}{a_1d_1^2}\right)_3^{-1}.
\end{aligned}$$

That is,

$$\left(\frac{ax+(b+1)y+2y\omega}{a_1d_1^2p}\right)_3 = \omega^{(r+t-s)B/3}\left(\frac{\omega}{2^{\alpha+2\beta}a_1d_1^2py_0}\right)_3^{j-k}. \tag{5.1}$$

Let us consider five cases.

Case 1: $y\equiv 0 \pmod 3$. Since $p=ax^2+2bxy+cy^2\equiv ax^2 \pmod 3$ we have $ax\not\equiv 0 \pmod 3$ and so $r=0$. Clearly $\pi'=-\left(\frac{-3}{ax}\right)\pi$. Hence $j=k=0$ and $B=-2\left(\frac{-3}{ax}\right)y$. From (5.1) we see that

$$\left(\frac{ax+(b+1)y+2y\omega}{a_1d_1^2p}\right)_3 = \omega^{-(\frac{-3}{ax})\frac{2y}{3}(t-s)} = \omega^{(1-s)(\frac{-3}{ax})\frac{y}{3}}.$$

Case 2: $a\equiv 0 \pmod 3$. In this case, $y\not\equiv 0 \pmod 3$. Since $(a,d+3)=1$ we have $b^2=ac-3+(d+3)\not\equiv 0 \pmod 3$ and so $ax+by\not\equiv 0 \pmod 3$.

If $y\not\equiv 0\pmod 3$, $x\equiv uy\pmod 9$ and $ax+by\not\equiv 0\pmod 3$, then clearly

$$\pi'=\begin{cases}-\left(\dfrac{-3}{y}\right)\omega\pi=\left(\dfrac{-3}{y}\right)(2y+(-ax-by+y)\omega)\\ \qquad\qquad\qquad\qquad\qquad\qquad\text{if } au+b\equiv 1\pmod 3,\\ \left(\dfrac{-3}{y}\right)\omega^2\pi=\left(\dfrac{-3}{y}\right)(-ax-by+y-(ax+by+y)\omega)\\ \qquad\qquad\qquad\qquad\qquad\qquad\text{if } au+b\equiv -1\pmod 3.\end{cases}$$

From this and (5.1) it follows that

$$\begin{aligned}&\left(\frac{ax+(b+1)y+2y\omega}{a_1d_1^2p}\right)_3\\ &\quad=\begin{cases}\left(\dfrac{\omega}{2^{\alpha+2\beta}a_1d_1^2py}\right)_3^2\omega^{(\frac{-3}{y})(-ax-by+y)(r-s)/3} & \text{if } au+b\equiv 1\pmod 3,\\ \left(\dfrac{\omega}{2^{\alpha+2\beta}a_1d_1^2py}\right)_3\omega^{-(\frac{-3}{y})(ax+by+y)(r-s)/3} & \text{if } au+b\equiv -1\pmod 3\end{cases}\\ &\quad=\left(\frac{\omega}{2^{\alpha+2\beta}a_1d_1^2py}\right)_3^{-(\frac{-3}{au+b})}\omega^{(au+b-(\frac{-3}{au+b}))(s-r)/3}.\end{aligned}$$

Observing that

$$\begin{aligned}py&=\left(a\left(\frac{x}{y}\right)^2+2b\frac{x}{y}+c\right)\left(3\cdot\frac{y-\left(\frac{-3}{y}\right)}{3}+\left(\frac{-3}{y}\right)\right)^3\\ &\equiv(au^2+2bu+c)\left(\frac{-3}{y}\right)\pmod 9,\end{aligned}$$

we get

$$\begin{aligned}&\left(\frac{ax+(b+1)y+2y\omega}{a_1d_1^2p}\right)_3\\ &\quad=\omega^{(au+b-(\frac{-3}{au+b}))(s-r)/3}\left(\frac{\omega}{2^{\alpha+2\beta}a_1d_1^2(au^2+2bu+c)}\right)_3^{-(\frac{-3}{au+b})}.\end{aligned}\tag{5.2}$$

Since $a\equiv 0\pmod 3$ we must have $d+3\not\equiv 0\pmod 3$ and so $d=b^2-ac\equiv 1\pmod 3$. Hence,

$$\left(\frac{\omega}{2^{2\beta}d_1^2}\right)_3=\left(\frac{\omega}{d+3}\right)_3^2=\omega^{2(1-d-3)/3}=\omega^{(d-1)/3+1}$$

and

$$\begin{aligned}\left(\frac{\omega}{2^{\alpha+2\beta}a_1d_1^2(au^2+2bu+c)}\right)_3&=\left(\frac{\omega}{2^\alpha a_1}\right)_3\left(\frac{\omega}{2^{2\beta}d_1^2}\right)_3\left(\frac{\omega}{au^2+2bu+c}\right)_3\\ &=\omega^{\frac13(1-(\frac{-3}{2^\alpha a_1})2^\alpha a_1)}\cdot\omega^{\frac{d-1}{3}+1}\cdot\omega^{\frac13(1-(\frac{-3}{2bu+c})(au^2+2bu+c))}.\end{aligned}$$

In view of (5.2),

$$\left(\frac{ax+(b+1)y+2y\omega}{a_1d_1^2p}\right)_3=\omega^{n_1},$$

where

$$\begin{aligned}n_1=&-r\frac{au+b-\left(\frac{-3}{au+b}\right)}{3}-\left(\frac{-3}{au+b}\right)\left(\frac{1}{3}\left(1-\left(\frac{-3}{2^\alpha a_1}\right)2^\alpha a_1\right)\right.\\&\left.+\frac{d-1}{3}+1+\frac{1}{3}\left(1-\left(\frac{-3}{2bu+c}\right)(au^2+2bu+c)\right)\right)\\=&-\frac{1}{3}\left(r\left(au+b-\left(\frac{-3}{b}\right)\right)+\left(\frac{-3}{b}\right)\left(d+3-\left(\frac{-3}{2^\alpha a_1}\right)2^\alpha a_1\right)\right.\\&\left.+\left(\frac{-3}{b}\right)\left(1-\left(\frac{-3}{2bu+c}\right)(au^2+2bu+c)\right)\right).\end{aligned}$$

Since

$$rau-\left(\frac{-3}{b}\right)\left(\frac{-3}{2bu+c}\right)au^2=au\left(r-\left(\frac{-3}{bc-u}\right)u\right)$$

$$\equiv\begin{cases}0\pmod 9 & \text{if } a\equiv 0\pmod 9 \text{ or } u\equiv 0\pmod 3,\\ a(-bc)\left(1-\left(\frac{-3}{2bc}\right)(-bc)\right)\equiv 0\pmod 9 & \\ & \text{if } a\equiv\pm 3\pmod 9 \text{ and } u\equiv -bc\pmod 3\end{cases}$$

and

$$d+3=b^2-1-ac+4\equiv 1-b\left(\frac{-3}{b}\right)-ac+4\pmod 9,$$

we see that $n_1\equiv f_1(u)\pmod 3$ and so

$$\left(\frac{ax+(b+1)y+2y\omega}{a_1d_1^2p}\right)_3=\omega^{f_1(u)}.$$

Case 3: $a(ax+by)\not\equiv 0\pmod 3$. In this case, $r=0$. Suppose $x\equiv uy\pmod 9$. Then

$$\begin{aligned}2^\alpha a_1(au^2+2bu+c)&=a^2u^2+2abu+ac\\&=\left(3\cdot\frac{au+b-\left(\frac{-3}{au+b}\right)}{3}+\left(\frac{-3}{au+b}\right)\right)^2-d\\&\equiv 1-d-\left((au+b)\left(\frac{-3}{au+b}\right)-1\right)\pmod 9.\end{aligned}$$

From this and (5.2) it follows that

$$\left(\frac{ax+(b+1)y+2y\omega}{a_1d_1^2p}\right)_3$$
$$=\left(\frac{\omega}{2^{2\beta}d_1^2\big(1-d-\big((au+b)\big(\frac{-3}{au+b}\big)-1\big)\big)}\right)_3^{-(\frac{-3}{au+b})}\omega^{s(au+b-(\frac{-3}{au+b}))/3}=\omega^{n_2},$$

where

$$\begin{aligned}n_2=&-\frac{1}{3}\left(\frac{-3}{au+b}\right)\left(1-\left(\frac{-3}{1-d}\right)2^{2\beta}d_1^2\right.\\&\left.\times\left(1-d-\left((au+b)\left(\frac{-3}{au+b}\right)-1\right)\right)\right)+\frac{s\big(au+b-\big(\frac{-3}{au+b}\big)\big)}{3}\\=&\frac{1}{3}\left(\frac{-3}{au+b}\right)\left(\left((au+b)\left(\frac{-3}{au+b}\right)-1\right)\right.\\&\left.\times\left(s-\left(\frac{-3}{1-d}\right)\right)+(2^\beta d_1)^2(1-d)\left(\frac{-3}{1-d}\right)-1\right).\end{aligned}$$

Since

$$\begin{aligned}&(2^\beta d_1)^2(1-d)\left(\frac{-3}{1-d}\right)-1\\&\quad=((2^\beta d_1)^2-1)\left((1-d)\left(\frac{-3}{1-d}\right)-1\right)+(1-d)\left(\frac{-3}{1-d}\right)+(2^\beta d_1)^2-2\\&\quad\equiv(1-d)\left(\frac{-3}{1-d}\right)-2^\beta d_1\left(\frac{-3}{2^\beta d_1}\right)\pmod 9,\end{aligned}$$

we obtain

$$\left(\frac{ax+(b+1)y+2y\omega}{a_1d_1^2p}\right)_3=\omega^{n_2}=\omega^{f_2(u)}.$$

Case 4: $ax+by\equiv 0\pmod 9$. Since $ax+by\equiv 0\pmod 3$ we have $ap=(ax+by)^2-dy^2\equiv -dy^2\pmod 9$. We claim that $ady\not\equiv 0\pmod 3$ and so that $r=s=t=0$.

If $y\equiv 0\pmod 3$ then

$$p=ax^2+2bxy+cy^2=(ax+by)x+(bx+cy)y\equiv 0\pmod 3.$$

Thus, $y\not\equiv 0\pmod 3$.

If $a\equiv 0\pmod 3$ then $dy^2\equiv -ap\equiv 0\pmod 3$. Since $y\not\equiv 0\pmod 3$ we have $d\equiv 0\pmod 3$ and so $d+3\equiv 0\pmod 3$. This contradicts the assumption $(a,d+3)=1$. Hence, $a\not\equiv 0\pmod 3$.

By the above, $ay\not\equiv 0\pmod 3$ and $dy^2\equiv -ap\pmod 9$. So $d\not\equiv 0\pmod 3$. This proves the assertion.

Now, it is easy to check that

$$\pi'=-\left(\frac{-3}{y}\right)\frac{\pi}{\omega(1-\omega)}=\left(\frac{-3}{y}\right)\left(-y+\frac{ax+by}{3}+\frac{2(ax+by)}{3}\omega\right).$$

So we have

$$r=s=t=0,\quad j=k=1\quad\text{and}\quad B=\left(\frac{-3}{y}\right)\frac{2(ax+by)}{3}.$$

This together with (5.1) gives

$$\left(\frac{ax+(b+1)y+2y\omega}{a_1d_1^2p}\right)_3=\omega^0=1.$$

Case 5: $ax+by\equiv\pm3y\pmod 9$. In this case, $ax+by\equiv 0\pmod 3$. By the above claim we have $r=s=t=0$. It is clear that

$$\pi'=\begin{cases}-\left(\dfrac{-3}{y}\right)\dfrac{\pi}{\omega^2(1-\omega)}=\left(\dfrac{-3}{y}\right)\left(\dfrac{ax+by}{3}+y+\left(y-\dfrac{ax+by}{3}\right)\omega\right)\\ \qquad\qquad\text{if } ax+by\equiv 3y\pmod 9,\\ -\left(\dfrac{-3}{y}\right)\dfrac{\pi}{1-\omega}=-\left(\dfrac{-3}{y}\right)\left(\dfrac{2(ax+by)}{3}+\left(\dfrac{ax+by}{3}+y\right)\omega\right)\\ \qquad\qquad\text{if } ax+by\equiv -3y\pmod 9.\end{cases}$$

Thus, by (5.1),

$$\left(\frac{ax+(b+1)y+2y\omega}{a_1d_1^2p}\right)_3=\begin{cases}\left(\dfrac{\omega}{2^{\alpha+2\beta}a_1d_1^2py}\right)_3^{2-1} & \text{if } ax+by\equiv 3y\pmod 9,\\ \left(\dfrac{\omega}{2^{\alpha+2\beta}a_1d_1^2py}\right)_3^{0-1} & \text{if } ax+by\equiv -3y\pmod 9.\end{cases}$$

Since

$$\begin{aligned}2^\alpha a_1(2^\beta d_1)^2py&=a(d+3)^2(ax^2+2bxy+cy^2)y\\&=(d+3)^2((ax+by)^2-dy^2)y\equiv(d^2-3d)(-d)y^3\\&=(-d^3+3d^2)y^3\equiv\left(-\left(\frac{-3}{d}\right)+3\right)\left(\frac{-3}{y}\right)\pmod 9,\end{aligned}$$

we obtain

$$\left(\frac{\omega}{2^{\alpha+2\beta}a_1d_1^2py}\right)_3=\left(\frac{\omega}{3-\left(\frac{-3}{d}\right)}\right)_3=\omega^{\frac{1}{3}(1-(3-(\frac{-3}{d}))(\frac{-3}{3-(\frac{-3}{d})}))}=\omega^{(\frac{-3}{d})}$$

and hence

$$\left(\frac{ax+(b+1)y+2y\omega}{a_1d_1^2p}\right)_3=\omega^{\pm(\frac{-3}{d})}.$$

This completes the proof.

From Theorem 5.1 we have

THEOREM 5.2. *Let p be a prime greater than 3, $d \in \{-1,-2,-5,-6,-7,-15\}$, $\left(\frac{d}{p}\right)=1$ and $(s(d))^2 \equiv d \pmod p$. Then $s(d) \in C_0(p)$ if and only if p can be represented by one of the corresponding binary quadratic forms in Table* 5.1.

Table 5.1

d	*Binary quadratic forms*
-1	$x^2+81y^2,\ 2x^2+2xy+41y^2$
-2	$x^2+162y^2,\ 2x^2+81y^2$
-5	$x^2+405y^2, 5x^2+81y^2, 10x^2+10xy+43y^2, 2x^2+2xy+203y^2$
-6	$x^2+54y^2,\ 2x^2+27y^2$
-7	$x^2+567y^2,\ 7x^2+81y^2,\ 23x^2+20xy+29y^2$
-15	$x^2+135y^2,\ 5x^2+27y^2$

P r o o f. If $d=-1$ then $\left(\frac{-1}{p}\right)=1$ and so $p=x^2+y^2$ for some $x,y\in\mathbb{Z}$. Setting $a=1,\ b=0$ and $c=1$ in Theorem 5.1 we get

$$\left(\frac{x+y+2y\omega}{p}\right)_3=\begin{cases}\omega^{(\frac{-3}{x})\frac{y}{3}} & \text{if } 3\mid y,\\ \omega^{(u-(\frac{-3}{u}))/3} & \text{if } 3\nmid x \text{ and } x\equiv uy \pmod 9,\\ 1 & \text{if } 9\mid x,\\ \omega^{\mp 1} & \text{if } x\equiv \pm 3y \pmod 9.\end{cases}$$

Since $y\not\equiv 0 \pmod p$ and $s(-1)\equiv \pm x/y \pmod p$ we see that

$$\begin{aligned} s(-1)\in C_0(p) &\Leftrightarrow x/y\in C_0(p)\\ &\Leftrightarrow \left(\frac{x+y+2y\omega}{p}\right)_3=\left(\frac{x/y+1+2\omega}{p}\right)_3=1\\ &\Leftrightarrow 9\mid x,\ 9\mid y \text{ or } x\equiv\left(\frac{-3}{xy}\right)y \pmod 9.\end{aligned}$$

Clearly, $p=x^2+y^2$ with $x,y\in\mathbb{Z}$ and $9\mid xy$ if and only if $p=x_1^2+81y_1^2$ for some $x_1,y_1\in\mathbb{Z}$. If $p=x^2+y^2$ with $x\equiv\left(\frac{-3}{xy}\right)y \pmod 9$ then $p=2x_1^2+2x_1y_1+41y_1^2$ for $x_1=\frac{1}{9}\left(4x+5\left(\frac{-3}{xy}\right)y\right)$ and $y_1=\frac{1}{9}\left(x-\left(\frac{-3}{xy}\right)y\right)$. Conversely, if $p=2x_1^2+2x_1y_1+41y_1^2$ with $x_1,y_1\in\mathbb{Z}$ then $p=x^2+y^2$ for $x=x_1+5y_1$ and $y=x_1-4y_1$. Also, $x\equiv\left(\frac{-3}{xy}\right)y \pmod 9$.

By the above, $s(-1)\in C_0(p)$ if and only if $p=x^2+81y^2$ or $p=2x^2+2xy+41y^2$ for some $x,y\in\mathbb{Z}$.

If $d=-2$ then $\left(\frac{-2}{p}\right)=1$ and so $p=x^2+2y^2$ for some $x,y\in\mathbb{Z}$. Using the fact that $s(-2)\equiv\pm x/y \pmod p$ and Theorem 5.1 we see that

$$\begin{aligned} s(-2)\in C_0(p)\Leftrightarrow \left(\frac{x+y+2y\omega}{p}\right)_3=1 &\Leftrightarrow 9\mid x \text{ or } 9\mid y\\ &\Leftrightarrow p=x_1^2+162y_1^2 \text{ or } p=2x_1^2+81y_1^2\ (x_1,y_1\in\mathbb{Z}).\end{aligned}$$

If $d=-5$ then $\left(\frac{-5}{p}\right)=1$ and so $p=x^2+5y^2$ or $p=3x^2+2xy+2y^2$ for some $x,y\in\mathbb{Z}$. Using Theorem 5.1 we see that

$$s(-5)\in C_0(p)\Leftrightarrow\begin{cases}x/y\in C_0(p)\Leftrightarrow 9\mid x \text{ or } 9\mid y\\ \qquad\qquad\text{if } p=x^2+5y^2,\\ 1+3x/y\in C_0(p)\Leftrightarrow 9\mid x \text{ or } x\equiv -2y \pmod 9\\ \qquad\qquad\text{if } p=3x^2+2xy+2y^2.\end{cases}$$

This yields the result.

If $d=-6$ then $\left(\frac{-6}{p}\right)=1$ and so $p=x^2+6y^2$ or $p=2x^2+3y^2$ for some $x,y\in\mathbb{Z}$. Applying Theorem 5.1 we get

$$s(-6)\in C_0(p)\Leftrightarrow\begin{cases}x/y\in C_0(p)\Leftrightarrow 3\mid y & \text{if } p=x^2+6y^2,\\ 2x/y\in C_0(p)\Leftrightarrow 3\mid y & \text{if } p=2x^2+3y^2.\end{cases}$$

This gives the result.

If $d=-7$ then $\left(\frac{-7}{p}\right)=1$ and so $p=x^2+7y^2$ for some $x,y\in\mathbb{Z}$. Applying Theorem 5.1 we see that

$$s(-7)\in C_0(p)\Leftrightarrow x/y\in C_0(p)\Leftrightarrow 9\mid x,\ 9\mid y \text{ or } x\equiv 4\left(\frac{-3}{xy}\right)y \pmod 9.$$

This yields the desired result.

If $d=-15$ then $\left(\frac{-15}{p}\right)=1$ and hence $p=x^2+15y^2$ or $p=5x^2+3y^2$ for some $x,y\in\mathbb{Z}$. In view of Theorem 5.1 we get

$$s(-15)\in C_0(p)\Leftrightarrow\begin{cases}x/y\in C_0(p)\Leftrightarrow 3\mid y & \text{if } p=x^2+15y^2,\\ 5x/y\in C_0(p)\Leftrightarrow 3\mid y & \text{if } p=5x^2+3y^2.\end{cases}$$

This deduces the result.

Combining the above we prove the theorem.

Corollary 5.1. *Let p be a prime greater than* 3.

(i) *If $\left(\frac{-1}{p}\right)=1$ then $x^3+6x+4\equiv 0 \pmod p$ is solvable if and only if $p=x^2+81y^2$ or $p=2x^2+2xy+41y^2$ for some $x,y\in\mathbb{Z}$.*

(ii) *If $\left(\frac{-2}{p}\right)=1$ then $x^3-9x-18\equiv 0 \pmod p$ is solvable if and only if $p=x^2+162y^2$ or $p=2x^2+81y^2$ for some $x,y\in\mathbb{Z}$.*

(iii) *If $\left(\frac{-6}{p}\right)=1$ then $x^3+3x+2\equiv 0 \pmod p$ is solvable if and only if $p=x^2+54y^2$ or $p=2x^2+27y^2$ for some $x,y\in\mathbb{Z}$.*

(iv) *If $\left(\frac{-15}{p}\right)=1$ then $x^3+3x+1\equiv 0 \pmod p$ is solvable if and only if $p=x^2+135y^2$ or $p=5x^2+27y^2$ for some $x,y\in\mathbb{Z}$.*

Proof. If $\left(\frac{-1}{p}\right)=1$, then $(s(-1))^2\equiv -1 \pmod p$ for some $s(-1)\in\mathbb{Z}$. Set $a=-2$ and $b=2$. Then $(6s(-1))^2\equiv -3(b^2-4a) \pmod p$. From Theorems 4.1 and 5.2 we see that

$$x^3+6x+4\equiv 0\ (\mathrm{mod}\,p) \text{ is solvable} \Leftrightarrow 6s(-1)/2\in C_0(p)$$
$$\Leftrightarrow s(-1)\in C_0(p) \text{ (by Proposition 2.2(i))}$$
$$\Leftrightarrow p=x^2+81y^2 \text{ or } p=2x^2+2xy+41y^2\ (x,y\in\mathbb{Z}).$$

This proves (i).

Similarly, by using Theorems 4.1 and 5.2 one can prove (ii)–(iv).

REMARK 5.1. Kronecker [K] showed that $x^3+x+1\equiv 0\ (\mathrm{mod}\,p)$ is solvable for prime p satisfying $\left(\frac{-31}{p}\right)=1$ if and only if $p=x^2+31y^2$ for some integers x and y. In 1973, E. Lehmer [L3] proved Corollary 5.1(iv) in the case $p\equiv 1\ (\mathrm{mod}\,3)$. For recent important papers along this line one may consult [WH] and [SW].

COROLLARY 5.2. *Let p be a prime of the form $3n+1$, and ε_d denote the fundamental unit of the quadratic field $\mathbb{Q}(\sqrt{d})$.*

(i) *If $d\in\{2,3,5\}$ and $\left(\frac{d}{p}\right)=1$ then ε_d is a cubic residue (mod p) if and only if $p=x^2+27dy^2$ for some integers x and y.*

(ii) *If $\left(\frac{6}{p}\right)=1$ then $\varepsilon_6\ (=5+2\sqrt{6})$ is a cubic residue (mod p) if and only if $p=x^2+162y^2$ for some integers x and y.*

(iii) *If $\left(\frac{15}{p}\right)=1$ then $\varepsilon_{15}\ (=4+\sqrt{15})$ is a cubic residue (mod p) if and only if $p=x^2+405y^2$ or $p=10x^2+10xy+43y^2$ for some integers x and y.*

(iv) *If $\left(\frac{21}{p}\right)=1$ then $\varepsilon_{21}\ (=\frac{1}{2}(5+\sqrt{21}))$ is a cubic residue (mod p) if and only if $p=x^2+567y^2$ or $p=7x^2+81y^2$ for some integers x and y.*

Proof. Suppose $t^2\equiv -3\ (\mathrm{mod}\,p)$, $\left(\frac{-d}{p}\right)=1$ and $(s(-d))^2\equiv -d\ (\mathrm{mod}\,p)$. By Theorem 2.2(i), $s(-d)\in C_0(p)$ if and only if $(s(-d)-t)/(s(-d)+t)$ is a cubic residue (mod p). Observing that

$$\frac{s(-d)-t}{s(-d)+t}=\frac{(s(-d))^2-2s(-d)t+t^2}{(s(-d))^2-t^2}\equiv\frac{d+3+2s(-d)t}{d-3}\ (\mathrm{mod}\,p)$$

and that $(s(-d)t)^2\equiv 3d\ (\mathrm{mod}\,p)$ we find that

$$s(-d)\in C_0(p)\Leftrightarrow\frac{d+3+2\sqrt{3d}}{d-3}\text{ is a cubic residue (mod } p). \tag{5.3}$$

Clearly,

$$\varepsilon_2=1+\sqrt{2}=\frac{(1+\sqrt{2})^3}{3+2\sqrt{2}},\quad \varepsilon_3=2+\sqrt{3},$$
$$\varepsilon_5=\frac{1+\sqrt{5}}{2}=\left(\frac{1+\sqrt{5}}{2}\right)^3\Big/\left(\frac{3+\sqrt{5}}{2}\right),\quad \varepsilon_6=5+2\sqrt{6},$$
$$\varepsilon_{15}=4+\sqrt{15},\quad \varepsilon_{21}=\frac{1}{2}(5+\sqrt{21}).$$

Hence, combining Theorem 5.2 with (5.3) in the cases $d = 6, 1, 15, 2, 5, 7$ gives the result.

REMARK 5.2. Corollary 5.2(i) was known by E. Lehmer [L3], and the rest of Corollary 5.2 is new. For a general result on the cubic character of quadratic units one may consult [We].

THEOREM 5.3. *Let p be a prime of the form $3n+1$, $4p = L^2 + 27M^2$ $(L, M \in \mathbb{Z})$, and $q(d)$ $(q(d) > 3)$ a prime divisor of $L^2 - 9dM^2$ or $-dL^2 + 81M^2$.*

(i) *If $k \in \mathbb{Z}$ then $q(-3k^2)$ is a cubic residue (mod p) if and only if $(k-1)(k^2-1)$ is a cubic residue (mod $q(-3k^2)$).*

(ii) *If $d \in \{-1, -2, -5, -6, -7, -15\}$ then $q(d)$ is a cubic residue (mod p) if and only if $q(d)$ can be represented by one of the corresponding binary quadratic forms in Table* 5.1.

Proof. Suppose $(s(d))^2 \equiv d \pmod{q(d)}$. We first claim that

$$q(d) \text{ is a cubic residue } (\mathrm{mod}\ p) \Leftrightarrow s(d) \in C_0(q(d)). \tag{5.4}$$

If $q(d) \mid d$ then $q(d) \mid LM$ and $q(d) \mid s(d)$. From Proposition 2.1 and Corollary 2.1 we see that $s(d) \in C_0(q(d))$ and that $q(d)$ is a cubic residue (mod p).

If $q(d) \nmid d$ then $q(d) \nmid LM$. (Otherwise, $4p = L^2 + 27M^2 \equiv 0 \pmod{(q(d))^2}$.) Since

$$\left(\frac{L}{3M}\right)^2 \equiv d \pmod{q(d)} \quad \text{or} \quad \left(\frac{9M}{L}\right)^2 \equiv d \pmod{q(d)}$$

we have

$$s(d) \equiv \pm\frac{L}{3M} \quad \text{or} \quad s(d) \equiv \pm\frac{9M}{L} \pmod{q(d)}.$$

Now, applying Corollary 2.1 and Proposition 2.2(i) we see that

$$q(d) \text{ is a cubic residue } (\mathrm{mod}\ p) \Leftrightarrow \frac{L}{3M} \in C_0(q(d)) \Leftrightarrow s(d) \in C_0(q(d)).$$

This proves the assertion.

Now let us consider (i). Suppose $d = -3k^2$ for some $k \in \mathbb{Z}$. If $k \equiv \pm 1 \pmod{q(d)}$ then $d \equiv -3 \pmod{q(d)}$ and so $4p = L^2 + 27M^2 \equiv 0 \pmod{q(d)}$. This implies $q(d) = p$. So $q(d)$ is a cubic residue (mod p). If $k \not\equiv \pm 1 \pmod{q(d)}$, by (5.3) and (5.4) we see that

$$\begin{aligned} &q(d) \text{ is a cubic residue } (\mathrm{mod}\ p) \Leftrightarrow s(d) \in C_0(q(d)) \\ &\quad \Leftrightarrow \frac{3k^2 + 3 + 2 \cdot 3k}{3k^2 - 3} \left(= \frac{k+1}{k-1} \right) \text{ is a cubic residue } (\mathrm{mod}\ q(d)) \\ &\quad \Leftrightarrow (k-1)(k^2-1) \text{ is a cubic residue } (\mathrm{mod}\ q(d)). \end{aligned}$$

This proves (i).

(ii) follows from (5.4) and Theorem 5.2.

REMARK 5.3. When $q(d)$ is a prime divisor of L^2+9dM^2 Federighi and Roll [FR] conjectured Theorem 5.3(ii) in the cases $d=6,15$. Ph. Barkan [Ba] showed how to prove their conjecture about primes $q(d)\equiv 1 \pmod 3$.

In 1992, using class field theory Spearman and Williams [SW] proved the following important result:

(5.5) Suppose $p>3$ is a prime and x^3+Ax^2+Bx+C $(A,B,C\in\mathbb{Z})$ is irreducible over the rational field $\mathbb{Q}$. If the discriminant $D=A^2B^2-4B^3-4A^3C-27C^2+18ABC$ is not a perfect square such that $\left(\frac{D}{p}\right)=1$, and $H(D)$ is the form class group of classes of primitive, integral binary quadratic forms of discriminant D, then the cubic congruence $x^3+Ax^2+Bx+C\equiv 0 \pmod p$ is solvable if and only if p can be represented by one of the third (composition) powers of forms in $H(D)$.

From (5.5) we have

LEMMA 5.1. *Assume that $p>3$ is a prime, $m,n\in\mathbb{Z}$, $2\mid mn$, $p\nmid mn$, $m^3n\neq -2,4,64,108,250$, $m^3n/2-27\notin\{k^2\mid k\in\mathbb{Z}\}$ and $\left(\frac{m^3n/2-27}{p}\right)=1$. Then the cubic congruence $x^3-\frac{mn}{2}x-n\equiv 0 \pmod p$ is solvable if and only if p can be represented by one of the third powers of primitive integral binary quadratic forms of discriminant $(m^3n/2-27)n^2$.*

Proof. Clearly the discriminant of $x^3-\frac{mn}{2}x-n$ is given by

$$D=-4\left(-\frac{mn}{2}\right)^3-27(-n)^2=\left(\frac{m^3n}{2}-27\right)n^2.$$

Since D is not a square, by (5.5) it is sufficient to prove that $x^3-\frac{mn}{2}x-n\neq 0$ for any integer x.

If $t\in\mathbb{Z}$ and $t^3-\frac{mn}{2}t-n=0$, then $n=st$ for some $s\in\mathbb{Z}$. Since $n\not\equiv 0 \pmod p$ we have $st\neq 0$ and so $t^2-\frac{mst}{2}-s=0$. This implies $t\mid 2s$. Write $2s=rt$. Then $t^2-\frac{mr}{4}t^2-\frac{rt}{2}=0$. Namely, $4t-mrt-2r=0$. It then follows that $4t=kr$ for some $k\in\mathbb{Z}$. Observing that $r=2s/t\neq 0$ we find $k(4-mr)=8$ and hence $k\in\{\pm1,\pm2,\pm4,\pm8\}$. Since

$$m^3n=m^3\cdot\frac{r}{2}\cdot\left(\frac{kr}{4}\right)^2=\frac{(mr)^3}{32}k^2=\frac{k^2}{32}\left(4-\frac{8}{k}\right)^3=\frac{2(k-2)^3}{k}$$

and $k\in\{\pm1,\pm2,\pm4,\pm8\}$ we get $m^3n\in\{-2,54,0,64,4,108,250\}$. This contradicts the assumption. Thus, $x^3-\frac{mn}{2}x-n\neq 0$ for any $x\in\mathbb{Z}$. This completes the proof.

Now we can give

THEOREM 5.4. *If $p>3$ is a prime, $d\in\mathbb{Z}, d\neq 3, d\not\equiv -3 \pmod p, d\notin\{k^2\mid k\in\mathbb{Z}\}, \left(\frac{d}{p}\right)=1, (s(d))^2\equiv d \pmod p$ and $18(d+3)=m^3n$ with $m,n\in\mathbb{Z}$, then $s(d)\in C_0(p)$ if and only if p can be represented by one of*

the third powers of primitive integral binary quadratic forms of discriminant $9dn^2$.

P r o o f. It follows from Lemma 4.1 that

$$\begin{aligned} s(d) \in C_0(p) &\Leftrightarrow x^3 - 9((s(d))^2+3)x - 18((s(d))^2+3) \equiv 0 \pmod p \text{ is solvable} \\ &\Leftrightarrow x^3 - 9(d+3)x - 18(d+3) \equiv 0 \pmod p \text{ is solvable} \\ &\Leftrightarrow (my)^3 - \frac{m^3 n}{2} my - m^3 n \equiv 0 \pmod p \text{ is solvable} \\ &\Leftrightarrow y^3 - \frac{mn}{2} y - n \equiv 0 \pmod p \text{ is solvable.} \end{aligned}$$

Since $(m^3n/2 - 27)n^2 = 9dn^2$ and $m^3n = 18(d+3) \neq -2, 4, 64, 108, 250$, applying Lemma 5.1 we obtain the result.

Corollary 5.3. *If* p *is a prime,* $p \equiv 1 \pmod 3, k \in \mathbb{Z}, k \not\equiv 0, \pm 1 \pmod p$ *and* $2(k^2-1) = m^3 n$ $(m, n \in \mathbb{Z})$, *then* $\frac{k+1}{k-1}$ *is a cubic residue* (*mod* p) *if and only if* p *can be represented by one of the third powers of primitive integral binary quadratic forms of discriminant* $-27k^2n^2$.

P r o o f. Suppose $d = -3k^2$ and $t^2 \equiv -3 \pmod p$. Clearly, $\left(\frac{d}{p}\right) = 1$, $d \not\equiv -3 \pmod p$ and $(-kt)^2 \equiv d \pmod p$. By Theorem 2.2(i), $-kt \in C_0(p)$ if and only if $\frac{k+1}{k-1}$ $(= \frac{-kt-t}{-kt+t})$ is a cubic residue (mod p). Also, $18(d+3) = 18(3-3k^2) = (-3m)^3 n$ and $9dn^2 = -27k^2n^2$. So the result follows from Theorem 5.4.

Corollary 5.4. *Let* p *be a prime of the form* $3n+1, 4p = L^2 + 27M^2$ $(L, M \in \mathbb{Z}), d \in \mathbb{Z}, d \notin \{k^2 \mid k \in \mathbb{Z}\}, d \not\equiv 3, d \not\equiv -3 \pmod p$ *and* $18(d+3) = m^3 n$ $(m, n \in \mathbb{Z})$. *If* $q(d)$ *is a prime divisor of* $L^2 - 9dM^2$ *or* $-dL^2 + 81M^2$ *satisfying* $q(d) \neq 2, 3$ *and* $q(d) \nmid d$, *then* $q(d)$ *is a cubic residue* (*mod* p) *if and only if* $q(d)$ *can be represented by one of the third powers of primitive integral binary quadratic forms of discriminant* $9dn^2$.

P r o o f. This is immediate from (5.4) and Theorem 5.4.

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

$$\begin{aligned} &u_0(a,b) = 0, \quad u_1(a,b) = 1, \\ &u_{n+1}(a,b) = bu_n(a,b) - au_{n-1}(a,b) \quad (n \geq 1); \end{aligned} \tag{6.1}$$

$$\begin{aligned} &v_0(a,b) = 2, \quad v_1(a,b) = b, \\ &v_{n+1}(a,b) = bv_n(a,b) - av_{n-1}(a,b) \quad (n \geq 1). \end{aligned} \tag{6.2}$$

It is well known that

$$u_n(a,b)=\frac{1}{\sqrt{b^2-4a}}\left(\left(\frac{b+\sqrt{b^2-4a}}{2}\right)^n-\left(\frac{b-\sqrt{b^2-4a}}{2}\right)^n\right)\quad(b^2-4a\ne0) \tag{6.3}$$

and that

$$v_n(a,b)=\left(\frac{b+\sqrt{b^2-4a}}{2}\right)^n+\left(\frac{b-\sqrt{b^2-4a}}{2}\right)^n. \tag{6.4}$$

Suppose that p is a prime greater than 3. It is the purpose of this section to determine $u_{(p-(\frac{-3}{p}))/3}(a,b)\pmod p$ and $v_{(p-(\frac{-3}{p}))/3}(a,b)\pmod p$.

THEOREM 6.1. *Let $p>3$ be a prime, $a,b\in\mathbb{Z}_p, p\nmid ab, \left(\frac{-3(b^2-4a)}{p}\right)=1$ and $s^2\equiv-3(b^2-4a)\pmod p$. Then*

$$u_{(p-(\frac{-3}{p}))/3}(a,b)\equiv\begin{cases}0\pmod p & \text{if } s/b\in C_0(p),\\ \pm\dfrac{3}{s}(-a)^{-[p/3]}\pmod p & \text{if } \pm s/b\in C_1(p)\end{cases}$$

and

$$v_{(p-(\frac{-3}{p}))/3}(a,b)\equiv\begin{cases}2a^{-[p/3]}\pmod p & \text{if } s/b\in C_0(p),\\ -a^{-[p/3]}\pmod p & \text{if } s/b\notin C_0(p).\end{cases}$$

Proof. Set $k=-3b/s$. For $n\in\mathbb{Z}^+$ it is clear that

$$\begin{aligned}u_n(a,b)&=\frac{1}{\sqrt{b^2-4a}}\left(\left(\frac{b+\sqrt{b^2-4a}}{2}\right)^n-\left(\frac{b-\sqrt{b^2-4a}}{2}\right)^n\right)\\&=\frac{2}{2^n\sqrt{b^2-4a}}\sum_{r=0}^{[(n-1)/2]}\binom{n}{2r+1}b^{n-2r-1}(\sqrt{b^2-4a})^{2r+1}\\&=\frac{2}{2^n}\sum_{r=0}^{[(n-1)/2]}\binom{n}{2r+1}b^{n-2r-1}(b^2-4a)^r\\&\equiv\frac{2}{2^n}\sum_{r=0}^{[(n-1)/2]}\binom{n}{2r+1}b^{n-2r-1}\left(\frac{s(1+2\omega)}{-3}\right)^{2r+1}\frac{-3}{s(1+2\omega)}\\&=\frac{-3}{s(1+2\omega)}\left(\left(\frac{b+s(1+2\omega)/(-3)}{2}\right)^n-\left(\frac{b-s(1+2\omega)/(-3)}{2}\right)^n\right)\\&=\frac{\omega(1-\omega)}{s}\left(-\frac{s}{6}\right)^n((k+1+2\omega)^n-(k-1-2\omega)^n)\pmod p.\end{aligned}$$

Similarly,

$$\begin{aligned}v_n(a,b)&=\frac{2}{2^n}\sum_{r=0}^{[n/2]}\binom{n}{2r}b^{n-2r}(b^2-4a)^r\\&\equiv\frac{2}{2^n}\sum_{r=0}^{[n/2]}\binom{n}{2r}b^{n-2r}\left(\frac{s(1+2\omega)}{-3}\right)^{2r}\end{aligned}$$

$$= \left(\frac{b + s(1+2\omega)/(-3)}{2}\right)^n + \left(\frac{b - s(1+2\omega)/(-3)}{2}\right)^n$$
$$= \left(-\frac{s}{6}\right)^n ((k+1+2\omega)^n + (k-1-2\omega)^n) \pmod p.$$

If $p \equiv 1 \pmod 3$, we may write $p = \lambda\overline{\lambda}$ with $\lambda \in \mathbb{Z}[\omega]$ and $\lambda \equiv 2 \pmod 3$. By Lemma 2.2(i),

$$(k^2+3)^{(p-1)/3}((k-1-2\omega)^{(p-1)/3} \pm (k+1+2\omega)^{(p-1)/3})$$
$$\equiv \left(\frac{(k^2+3)(k-1-2\omega)}{\lambda}\right)_3 \pm \left(\frac{(k^2+3)(k+1+2\omega)}{\lambda}\right)_3$$
$$= \left(\frac{k+1+2\omega}{p}\right)_3 \pm \left(\frac{k+1+2\omega}{p}\right)_3^{-1} \pmod\lambda.$$

Hence, by the above and Fermat's little theorem we get

$$u_{(p-1)/3}(a,b) \equiv -\frac{\omega(1-\omega)}{s}\left(-\frac{s}{6}\right)^{(p-1)/3}(k^2+3)^{-(p-1)/3}$$
$$\times \left(\left(\frac{k+1+2\omega}{p}\right)_3 - \left(\frac{k+1+2\omega}{p}\right)_3^{-1}\right)$$
$$\equiv \begin{cases} 0 \pmod\lambda & \text{if } k \in C_0(p), \\ \pm\dfrac{3}{s}(-a)^{(p-1)/3} \pmod\lambda & \text{if } \pm k \in C_1(p) \end{cases}$$

and

$$v_{(p-1)/3}(a,b)$$
$$\equiv \left(-\frac{s}{6}\right)^{(p-1)/3}(k^2+3)^{-(p-1)/3}\left(\left(\frac{k+1+2\omega}{p}\right)_3 + \left(\frac{k+1+2\omega}{p}\right)_3^{-1}\right)$$
$$\equiv \begin{cases} 2a^{-(p-1)/3} \pmod\lambda & \text{if } k \in C_0(p), \\ -a^{-(p-1)/3} \pmod\lambda & \text{if } k \in C_1(p) \cup C_2(p). \end{cases}$$

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

If $p \equiv 2 \pmod 3$, it follows from Lemma 2.2(ii) that

$$(k+1+2\omega)^{(p+1)/3} \pm (k-1-2\omega)^{(p+1)/3}$$
$$\equiv (k^2+3)^{-(p-2)/3}\left(\left(\frac{k+1+2\omega}{p}\right)_3 \pm \left(\frac{k+1+2\omega}{p}\right)_3^{-1}\right) \pmod p.$$

From this and the above it follows that

$$u_{(p+1)/3}(a,b) \equiv \frac{\omega(1-\omega)}{s}\left(-\frac{s}{6}\right)^{(p+1)/3}(k^2+3)^{-(p-2)/3}$$
$$\times \left(\left(\frac{k+1+2\omega}{p}\right)_3 - \left(\frac{k+1+2\omega}{p}\right)_3^{-1}\right)$$

$$\equiv \begin{cases} 0 \pmod p & \text{if } k \in C_0(p), \\ \pm\dfrac{3}{s}(-a)^{-(p-2)/3} \pmod p & \text{if } \pm k \in C_1(p) \end{cases}$$

and

$$\begin{aligned} &v_{(p+1)/3}(a,b) \\ &\quad\equiv \left(-\frac{s}{6}\right)^{(p+1)/3}(k^2+3)^{-(p-2)/3}\left(\left(\frac{k+1+2\omega}{p}\right)_3+\left(\frac{k+1+2\omega}{p}\right)_3^{-1}\right) \\ &\quad\equiv \begin{cases} 2a^{-(p-2)/3} \pmod p & \text{if } k \in C_0(p), \\ -a^{-(p-2)/3} \pmod p & \text{if } k \in C_1(p)\cup C_2(p). \end{cases} \end{aligned}$$

To complete the proof, we note that

$$k^2+3 \equiv \frac{36a}{-3(b^2-4a)} \not\equiv 0 \pmod p$$

and $k \in C_i(p)$ if and only if $s/b \in C_i(p)$ by Proposition 2.2(i).

Corollary 6.1. *Let $p>3$ be a prime, $k \in \mathbb{Z}_p$ and $k(k^2+3) \not\equiv 0 \pmod p$. Then*

$$u_{(p-(\frac{-3}{p}))/3}(3k^2+9,6) \equiv \begin{cases} 0 \pmod p & \text{if } k \in C_0(p), \\ \dfrac{1}{2k}(-3k^2-9)^{-[p/3]} \pmod p & \text{if } k \in C_1(p), \\ -\dfrac{1}{2k}(-3k^2-9)^{-[p/3]} \pmod p & \text{if } k \in C_2(p) \end{cases}$$

and

$$v_{(p-(\frac{-3}{p}))/3}(3k^2+9,6) \equiv \begin{cases} 2(3k^2+9)^{-[p/3]} \pmod p & \text{if } k \in C_0(p), \\ -(3k^2+9)^{-[p/3]} \pmod p & \text{if } k \notin C_0(p). \end{cases}$$

Corollary 6.2. *Let $p>3$ be a prime, $d \in \mathbb{Z}_p$, $d \not\equiv -3 \pmod p$, $\left(\frac{d}{p}\right)=1$ and $(s(d))^2 \equiv d \pmod p$. Then $s(d) \in C_0(p)$ if and only if $u_{(p-(\frac{-3}{p}))/3}(3d+9,6) \equiv 0 \pmod p$.*

Proof. Set $k=s(d)$. Then $u_n(3k^2+9,6) \equiv u_n(3d+9,6) \pmod p$ by (6.1). Hence the result follows from Corollary 6.1.

Corollary 6.3. *Let $p>3$ be a prime, $a,b \in \mathbb{Z}_p$, $p \nmid ab$ and $\left(\frac{-3(b^2-4a)}{p}\right)=1$. Then the congruence $x^3-3ax-ab \equiv 0 \pmod p$ is solvable if and only if $u_{(p-(\frac{-3}{p}))/3}(a,b) \equiv 0 \pmod p$.*

Proof. Suppose $s^2 \equiv -3(b^2-4a) \pmod p$. It then follows from Theorem 6.1 that $s/b \in C_0(p)$ if and only if $u_{(p-(\frac{-3}{p}))/3}(a,b) \equiv 0 \pmod p$. This together with Theorem 4.1 gives the result.

Corollary 6.4. *Let $p>3$ be a prime, $a,b \in \mathbb{Z}$, $p \nmid ab$ and $\left(\frac{-3(b^2-4a)}{p}\right)=1$. If $-3(b^2-4a)$ is not a square and $x^3-3ax-ab$ is irreducible over*

$\mathbb{Q}$, *then* $p \mid u_{(p-(\frac{-3}{p}))/3}(a,b)$ *if and only if* p *can be represented by one of the third powers of primitive integral binary quadratic forms of discriminant* $-27a^2(b^2-4a)$.

Proof. Since the discriminant of $x^3 - 3ax - ab$ is $-27a^2(b^2-4a)$ the result follows from (5.5) and Corollary 6.3.

Let $\{F_n\}$ and $\{L_n\}$ be defined by

$$F_0 = 0, \quad F_1 = 1, \quad F_{n+1} = F_n + F_{n-1} \quad (n \geq 1)$$

and

$$L_0 = 2, \quad L_1 = 1, \quad L_{n+1} = L_n + L_{n-1} \quad (n \geq 1).$$

It is well known that $\{F_n\}$ is the Fibonacci sequence and that $\{L_n\}$ is the Lucas sequence.

From Theorems 5.1 and 6.1 we have

THEOREM 6.2. *Let* $p > 5$ *be a prime for which* $\left(\frac{-15}{p}\right) = 1$ *and hence* $p = x^2 + 15y^2$ *or* $p = 5x^2 + 3y^2$ *for some* $x, y \in \mathbb{Z}$ *according as* $p \equiv 1 \pmod 3$ *or* $p \equiv 2 \pmod 3$. *Then*

$$F_{(p-(\frac{-3}{p}))/3} \equiv \begin{cases} 0 \pmod p & \text{if } y \equiv 0 \pmod 3, \\ -\dfrac{x}{\left(2 + 3\left(\frac{-3}{p}\right)\right)y} \pmod p & \text{if } y \equiv x \pmod 3 \end{cases}$$

and

$$L_{(p-(\frac{-3}{p}))/3} \equiv \begin{cases} 2\left(\dfrac{-3}{p}\right) \pmod p & \text{if } y \equiv 0 \pmod 3, \\ -\left(\dfrac{-3}{p}\right) \pmod p & \text{if } y \not\equiv 0 \pmod 3. \end{cases}$$

Proof. Suppose $s = \left(3 - 2\left(\frac{-3}{p}\right)\right)\frac{x}{y}$. Then $s^2 \equiv -15 \pmod p$. Since $F_n = u_n(-1,1)$ and $L_n = v_n(-1,1)$, it follows from Theorem 6.1 that

$$F_{(p-(\frac{-3}{p}))/3} \equiv \begin{cases} 0 \pmod p & \text{if } s \in C_0(p), \\ \pm\dfrac{3}{s} \pmod p & \text{if } \pm s \in C_1(p) \end{cases}$$

and that

$$L_{(p-(\frac{-3}{p}))/3} \equiv \begin{cases} 2(-1)^{-[p/3]} = 2\left(\dfrac{-3}{p}\right) \pmod p & \text{if } s \in C_0(p), \\ -(-1)^{-[p/3]} = \left(\dfrac{-3}{p}\right) \pmod p & \text{if } s \notin C_0(p). \end{cases}$$

From Theorem 5.1 we know that

$$\left(\frac{s+1+2\omega}{p}\right)_3=\left(\frac{sy+y+2y\omega}{p}\right)_3=\begin{cases}1 & \text{if } y\equiv 0\ (\mathrm{mod}\,3),\\ \omega & \text{if } x\equiv\left(\dfrac{-3}{p}\right)y\ (\mathrm{mod}\,3),\\ \omega^2 & \text{if } x\equiv-\left(\dfrac{-3}{p}\right)y\ (\mathrm{mod}\,3).\end{cases}$$

Hence, $s\in C_0(p)$ if and only if $y\equiv 0\ (\mathrm{mod}\,3)$.

If $y\not\equiv 0\ (\mathrm{mod}\,3)$ then $x\equiv\pm\left(\frac{-3}{p}\right)y\ (\mathrm{mod}\,3)$ and so $\pm s\in C_1(p)$ by the above. Since

$$\frac{3}{s}=\frac{3y}{\left(3-2\left(\frac{-3}{p}\right)\right)x}\equiv-\frac{x}{\left(3+2\left(\frac{-3}{p}\right)\right)y}=-\left(\frac{-3}{p}\right)\frac{x}{\left(3\left(\frac{-3}{p}\right)+2\right)y}\ (\mathrm{mod}\,p)$$

we obtain

$$F_{(p-(\frac{-3}{p}))/3}\equiv\begin{cases}-\dfrac{x}{5y}\ (\mathrm{mod}\,p) & \text{if } p\equiv 1\ (\mathrm{mod}\,3) \text{ and } x\equiv y\ (\mathrm{mod}\,p),\\ \dfrac{x}{y}\ (\mathrm{mod}\,p) & \text{if } p\equiv 2\ (\mathrm{mod}\,3) \text{ and } x\equiv y\ (\mathrm{mod}\,p).\end{cases}$$

This completes the proof.

Lemma 6.1. *Let p be a prime greater than 3, $a,b\in\mathbb{Z}$, $u_n=u_n(a,b)$, $v_n=v_n(a,b)$ and $ab(b^2-4a)\not\equiv 0\ (\mathrm{mod}\,p)$. Then*

(a) *$p\mid u_{p-(\frac{-3}{p})}$ if and only if $\left(\frac{-3(b^2-4a)}{p}\right)=1$.*

(b) *$p\mid u_n$ if and only if $v_{2n}\equiv 2a^n\ (\mathrm{mod}\,p)$.*

Proof. From [D] and [R] we know that

$$u_{p-(\frac{b^2-4a}{p})}\equiv 0\ (\mathrm{mod}\,p),\quad u_p\equiv\left(\frac{b^2-4a}{p}\right)\ (\mathrm{mod}\,p). \tag{6.5}$$

Thus,

$$u_{p+(\frac{b^2-4a}{p})}=\begin{cases}bu_p-au_{p-1}\equiv b\ (\mathrm{mod}\,p) & \text{if } \left(\dfrac{b^2-4a}{p}\right)=1,\\ \dfrac{1}{a}(bu_p-u_{p+1})\equiv-\dfrac{b}{a}\ (\mathrm{mod}\,p) & \text{if } \left(\dfrac{b^2-4a}{p}\right)=-1\end{cases}$$
$$\not\equiv 0\ (\mathrm{mod}\,p).$$

It then follows that

$$p\mid u_{p-(\frac{-3}{p})}\Leftrightarrow\left(\frac{-3}{p}\right)=\left(\frac{b^2-4a}{p}\right)\Leftrightarrow\left(\frac{-3(b^2-4a)}{p}\right)=1.$$

This proves part (a).

Now consider part (b). According to [D] and [R] we have

$$u_{2n}=u_nv_n,\quad v_{2n}=v_n^2-2a^n, \tag{6.6}$$

$$v_n^2 - (b^2 - 4a)u_n^2 = 4a^n. \tag{6.7}$$

Thus,

$$p \mid u_n \Leftrightarrow v_n^2 \equiv 4a^n \pmod p \Leftrightarrow v_{2n} \equiv 2a^n \pmod p.$$

This concludes the proof.

Using Lemma 6.1 and Theorem 6.2 we have

Corollary 6.5. *Let p be a prime greater than* 5. *Then*

(i) $p \mid F_{(p-(\frac{-3}{p}))/3}$ *if and only if p can be represented by* $x^2 + 135y^2$ *or* $5x^2 + 27y^2$ *according as* $p \equiv 1 \pmod 3$ *or* $p \equiv 2 \pmod 3$.

(ii) $p \mid F_{(p-(\frac{-3}{p}))/6}$ *if and only if p can be represented by* $x^2 + 540y^2$ *or* $5x^2 + 108y^2$ *according as* $p \equiv 1 \pmod 3$ *or* $p \equiv 2 \pmod 3$.

Proof. It is well known that (see [D], [SS], [R]) $F_n \mid F_{mn}$ for $m, n \in \mathbb{Z}^+$. Thus $F_{(p-(\frac{-3}{p}))/3} \mid F_{p-(\frac{-3}{p})}$. If $p \mid F_{(p-(\frac{-3}{p}))/3}$ then $p \mid F_{p-(\frac{-3}{p})}$. Applying Lemma 6.1 we find $\left(\frac{-15}{p}\right) = 1$ and so $p = A^2 + 15B^2$ or $p = 5A^2 + 3B^2$ for some $A, B \in \mathbb{Z}$. It then follows from Theorem 6.2 that $3 \mid B$. Hence $p = x^2 + 135y^2$ or $p = 5x^2 + 27y^2$ for some $x, y \in \mathbb{Z}$.

Conversely, if p is represented by $x^2 + 135y^2$ or $5x^2 + 27y^2$, then $\left(\frac{-15}{p}\right) = 1$. Applying Theorem 6.2 we find $p \mid F_{(p-(\frac{-3}{p}))/3}$. This proves (i).

Let us consider (ii). If $p \mid F_{(p-(\frac{-3}{p}))/6}$ then $p \mid F_{p-(\frac{-3}{p})}$ and so $\left(\frac{-15}{p}\right) = 1$ by Lemma 6.1. If p is represented by $x^2 + 540y^2$ or $5x^2 + 108y^2$, we also have $\left(\frac{-15}{p}\right) = 1$. Hence, we may assume $\left(\frac{-15}{p}\right) = 1$ and so $p = x^2 + 15y^2$ or $p = 5x^2 + 3y^2$ for some $x, y \in \mathbb{Z}$. It then follows from Lemma 6.1 and Theorem 6.2 that

$$\begin{aligned}
p \mid F_{(p-(\frac{-3}{p}))/6} &\Leftrightarrow L_{(p-(\frac{-3}{p}))/3} \equiv 2(-1)^{(p-(\frac{-3}{p}))/6} \pmod p \\
&\Leftrightarrow (-1)^{(p-(\frac{-3}{p}))/6} = \left(\frac{-3}{p}\right) \text{ and } 3 \mid y \\
&\Leftrightarrow p = \begin{cases} A^2 + 135B^2 \equiv 1 \pmod{12}\ (A, B \in \mathbb{Z}) & \text{if } p \equiv 1 \pmod 3, \\ 5A^2 + 27B^2 \equiv 5 \pmod{12}\ (A, B \in \mathbb{Z}) & \text{if } p \equiv 2 \pmod 3 \end{cases} \\
&\Leftrightarrow p = A^2 + 135B^2 \text{ or } p = 5A^2 + 27B^2 \text{ with } B \equiv 0 \pmod 2 \\
&\Leftrightarrow p = x^2 + 540y^2 \text{ or } p = 5x^2 + 108y^2 \text{ for some } x, y \in \mathbb{Z}.
\end{aligned}$$

This completes the proof.

Remark 6.1. In [L3], [L4] E. Lehmer proved Corollary 6.5(i) in the case $p \equiv 1 \pmod{12}$. For the criteria for $p \mid F_{(p-1)/4}$ (if $p \equiv 1 \pmod 4$ is a prime) one may consult [L6], [SS].

Now we point out similar results for the Pell sequence. The *Pell sequence* $\{P_n\}$ and its companion $\{Q_n\}$ are given by

$$P_0=0,\quad P_1=1,\quad P_{n+1}=2P_n+P_{n-1}\quad (n\ge 1)$$

and

$$Q_0=2,\quad Q_1=2,\quad Q_{n+1}=2Q_n+Q_{n-1}\quad (n\ge 1).$$

Clearly, $P_n=u_n(-1,2)$ and $Q_n=v_n(-1,2)$.

Using Theorems 6.1 and 5.1 one can similarly prove

THEOREM 6.3. *Let $p>3$ be a prime such that $\left(\frac{-6}{p}\right)=1$ and hence $p=x^2+6y^2$ or $p=2x^2+3y^2$ for some $x,y\in\mathbb{Z}$ according as $p\equiv 1 \pmod 3$ or $p\equiv 2 \pmod 3$. Then*

$$P_{(p-(\frac{-3}{p}))/3}\equiv\begin{cases}0 \pmod p & \text{if } y\equiv 0 \pmod 3,\\ \dfrac{x}{\left(1+3\left(\frac{-3}{p}\right)\right)y} \pmod p & \text{if } y\equiv x \pmod 3\end{cases}$$

and

$$Q_{(p-(\frac{-3}{p}))/3}\equiv\begin{cases}2\left(\dfrac{-3}{p}\right) \pmod p & \text{if } y\equiv 0 \pmod 3,\\ -\left(\dfrac{-3}{p}\right) \pmod p & \text{if } y\not\equiv 0 \pmod 3.\end{cases}$$

REMARK 6.2. For the values of $P_{(p-1)/2} \pmod p$ and $P_{(p+1)/2} \pmod p$ one may consult [S1].

COROLLARY 6.6. *Let p be a prime greater than 3. Then*

(i) $p\mid P_{(p-(\frac{-3}{p}))/3}$ *if and only if $p=x^2+54y^2$ or $p=2x^2+27y^2$ for some integers x and y according as $p\equiv 1 \pmod 3$ or $p\equiv 2 \pmod 3$.*

(ii) $p\mid P_{(p-(\frac{-3}{p}))/6}$ *if and only if $p=x^2+216y^2$ or $p=8x^2+8xy+29y^2$ for some integers x and y according as $p\equiv 1 \pmod 3$ or $p\equiv 2 \pmod 3$.*

The proof of Corollary 6.6 is similar to the proof of Corollary 6.5.

REMARK 6.3. Let $p\equiv 1 \pmod 4$ be a prime. From [L4], [S1] we know that $p\mid P_{(p-1)/4}$ if and only if $p=x^2+32y^2$ for some integers x and y.

Finally, we discuss the Lucas sequence $\{u_n(1,4)\}$.

THEOREM 6.4. *Let $p\equiv 1 \pmod 4$ be a prime and hence $p=x^2+y^2$ for some integers x and y. Then*

$$u_{(p-(\frac{-3}{p}))/6}(1,4)$$
$$= 2^{-(p-(\frac{-3}{p}))/6} u_{(p-(\frac{-3}{p}))/3}(-2,2)$$
$$\equiv \begin{cases} 0 \pmod p & \text{if } 9 \mid xy(x^2-y^2), \\ -\dfrac{1}{2}\left(\dfrac{2}{p}\right)\dfrac{x}{y} \pmod p & \text{if } x \equiv 2y, -3y, 4y \pmod 9 \text{ or } y \equiv 3x \pmod 9 \end{cases}$$

and

$$v_{(p-(\frac{-3}{p}))/6}(1,4) = 2^{-(p-(\frac{-3}{p}))/6} v_{(p-(\frac{-3}{p}))/3}(-2,2)$$
$$\equiv \begin{cases} 2\left(\dfrac{-6}{p}\right) \pmod p & \text{if } 9 \mid xy(x^2-y^2), \\ -\left(\dfrac{-6}{p}\right) \pmod p & \text{if } 9 \nmid xy(x^2-y^2). \end{cases}$$

P r o o f. By (6.3) and (6.4) we have

$$2^n u_n(1,4) = \frac{1}{2\sqrt{3}}((4+2\sqrt{3})^n - (4-2\sqrt{3})^n)$$
$$= \frac{1}{2\sqrt{3}}((1+\sqrt{3})^{2n} - (1-\sqrt{3})^{2n}) = u_{2n}(-2,2)$$

and

$$2^n v_n(1,4) = (4+2\sqrt{3})^n + (4-2\sqrt{3})^n$$
$$= (1+\sqrt{3})^{2n} + (1-\sqrt{3})^{2n} = v_{2n}(-2,2).$$

Since $\frac{3x}{y} \cdot \frac{x}{y} \equiv -3 \pmod p$ it follows from Proposition 2.2(i) that $x/y \in C_i(p)$ if and only if $3x/y \in C_i(p)$. Thus, from $(6x/y)^2 \equiv -3(2^2 - 4(-2)) \pmod p$ and Theorem 6.1 we get

$$u_{(p-(\frac{-3}{p}))/3}(-2,2) \equiv \begin{cases} 0 \pmod p & \text{if } x/y \in C_0(p), \\ \pm\dfrac{y}{2x} \cdot 2^{-[p/3]} \pmod p & \text{if } \pm x/y \in C_1(p) \end{cases}$$

and

$$v_{(p-(\frac{-3}{p}))/3}(-2,2) \equiv \begin{cases} 2 \cdot (-2)^{-[p/3]} \pmod p & \text{if } x/y \in C_0(p), \\ -(-2)^{-[p/3]} \pmod p & \text{if } x/y \notin C_0(p). \end{cases}$$

From the proof of Theorem 5.2 we see that

$$x/y \in C_0(p) \Leftrightarrow 9 \mid xy(x^2-y^2)$$

and that

$$x/y \in C_1(p) \Leftrightarrow x \equiv 2y, -3y, 4y \pmod 9 \text{ or } y \equiv 3x \pmod 9.$$

Now, combining the above with the facts that

$$(-1)^{[p/3]}=\left(\frac{-3}{p}\right)\quad\text{and}\quad 2^{-(p-(\frac{-3}{p}))/6}\cdot 2^{-[p/3]}=2^{-(p-1)/2}\equiv\left(\frac{2}{p}\right)\pmod p$$

yields the desired result.

Corollary 6.7. *Let $p>3$ be a prime. Then $p\mid u_{(p-(\frac{-3}{p}))/6}(1,4)$ (or $p\mid u_{(p-(\frac{-3}{p}))/3}(-2,2)$) if and only if p can be represented by x^2+81y^2 or $2x^2+2xy+41y^2$ according as $p\equiv 1\pmod 3$ or $p\equiv 2\pmod 3$.*

Remark 6.4. Let $p>3$ be a prime. Using the method in the proof of Corollary 6.5(ii) one can similarly prove that $p\mid u_{(p-(\frac{-3}{p}))/6}(-2,2)$ if and only if p can be represented by $16x^2+81y^2$, $x^2+1296y^2$, $8x^2+8xy+41y^2$ or $32x^2-8xy+41y^2$.

Acknowledgements. I am grateful to the referee for suggesting many additional references.

References

[Ba] Ph. Barkan, *Partitions quadratiques et cyclotomie*, Sém. Delange–Pisot–Poitou (1975), Zbl324:10037.

[Bu] K. Burde, *Zur Herleitung von Reziprozitätsgesetzen unter Benutzung von endlichen Körpern*, J. Reine Angew. Math. 293/294 (1977), 418–427, MR57:16178.

[Ca] C. Cailler, *Sur les congruences du troisième degré*, Enseign. Math. 10 (1908), 474–487.

[C] A. Cauchy, *Sur la résolution des équivalences dont les modules se réduisent à des nombres premiers*, Exercises de Mathématiques 4 (1829), 253–292.

[CG] A. Cunningham and T. Gosset, *4-tic and 3-bic residuacity-tables*, Messenger Math. 50 (1920), 1–30.

[D] L. E. Dickson, *History of the Theory of Numbers*, Vol. I, Chelsea, New York, 1952, 393–407.

[FR] E. T. Federighi and R. G. Roll, Fibonacci Quart. (1966), 85–88.

[HW] R. H. Hudson and K. S. Williams, *Resolution of ambiguities in the evaluation of cubic and quartic Jacobsthal sums*, Pacific J. Math. 99 (1982), 379–386.

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

[J] J. G. D. Jacobi, *De residuis cubicis commentatio numerosa*, J. Reine Angew. Math. 2 (1827), 66–69.

[K] L. Kronecker, *Werke*, Vol. II, 93 and 97–101; Vol. IV, 123–129, Chelsea, New York, 1968.

[L1] E. Lehmer, *Criteria for cubic and quartic residuacity*, Mathematika 5 (1958), 20–29.

[L2] —, *On Euler's criterion*, J. Austral. Math. Soc. 1 (1959/1961, part 1), 64–70, MR21:7191.

[L3] —, *On the cubic character of quadratic units*, J. Number Theory 5 (1973), 385–389, MR48:271.

[L4] E. Lehmer, *On the quartic character of quadratic units*, J. Reine Angew. Math. 268/269 (1974), 294–301.

[L5] —, *On the number of solutions of* $u^k + D \equiv w \pmod p$, Pacific J. Math. 5 (1955), 103–118.

[L6] —, *On the quadratic character of the Fibonacci root*, Fibonacci Quart. 4 (1966), 135–138, MR39:160.

[Li] H. von Lienen, *Reelle kubische und biquadratische Legendre-Symbole*, J. Reine Angew. Math. 305 (1979), 140–154.

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

[Sh] D. Shanks, *On Gauss and composition I*, in: Number Theory and Applications (edited by R. A. Mollin), Dordrecht, Boston, 1989, 163–178, MR92e:11150.

[SW] B. K. Spearman and K. S. Williams, *The cubic congruence* $x^3+Ax^2+Bx+C \equiv 0 \pmod p$ *and binary quadratic forms*, J. London Math. Soc. (2) 46 (1992), 397–410, MR93j:11004.

[St] L. Stickelberger, *Über eine neue Eigenschaft der Diskriminanten algebraischer Zahlkörper*, Verhand. I. Internat. Math. Kongress (1897), Zürich, 182–193.

[S1] Z. H. Sun, *Combinatorial sum* $\sum_{\substack{k=0\\k\equiv r \pmod m}}^{n} \binom{n}{k}$ *and its applications in number theory II*, J. Nanjing Univ. Biquarterly 10 (1993), 105–118, MR94j:11021.

[S2] —, *Supplements to the theory of biquadratic residues*, submitted.

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

[We] P. J. Weinberger, *The cubic character of quadratic units*, Proc. 1972 Number Theory Conference, Univ. of Colorado, 1972, 241–242, MR52:10673.

[W1] K. S. Williams, *On Euler's criterion for cubic non-residues*, Proc. Amer. Math. Soc. 49 (1975), 277–283.

[W2] —, *Cubic nonresidues* (*mod p*), Delta 6 (1976), 23–28, MR54:5095.

[WH] K. S. Williams and R. H. Hudson, *Representation of primes by the principal form of discriminant* $-D$ *when the class number* $h(-D)$ *is* 3, Acta Arith. 57 (1991), 131–153.

Department of Mathematics
Huaiyin Teachers College
Huaiyin 223001, Jiangsu, People's Republic of China
E-mail: zwsun@netra.nju.edu.cn

Received on 21.11.1994
and in revised form on 8.9.1997 (2700)