Cubic, quartic, octic residues and Lucas sequences

Zhi-Hong Sun(孙智宏)
Huaiyin Normal University
Huaian, Jiangsu 223001, PR China
http://www.hytc.edu.cn/xsjl/szh

Notation: $\mathbb{Z}$—the set of integers, $\mathbb{N}$—the set of positive integers, $[x]$— the greatest integer not exceeding x, $\{x\}$—the fractional part of x, $(\frac{a}{m})$—the (quadratic) Jacobi symbol, $(\frac{\alpha}{\pi})_3$—the cubic Jacobi symbol,$(\frac{\alpha}{\pi})_4$—the quartci Jacobi symbol, $\mathbb{Z}_p$—the set of rational $p-$adic integers, $\text{ord}_p m$—the nonnegative integer α such that $p^\alpha \mid m$ but $p^{\alpha+1} \nmid m$, (a,b)—the greatest common divisor of a and b.

My related papers:

[S1] Z.H. Sun, Notes on quartic residue symbol and rational reciprocity laws, J. Nanjing Univ. Math. Biquarterly 9(1992), 92-101.

[S2] Z.H. Sun, On the theory of cubic resides and nonresidues, Acta Arith. 84(1998), 291-335.

[S3] Z.H. Sun, Supplements to the theory of quartic residues, Acta Arith. 97(2001), 361-377.

[S4] Z.H. Sun, Values of Lucas sequences modulo primes, Rocky Mountain J. Math. 33(2003), 1123-1145.

[S5] Z.H. Sun, Cubic and quartic congruences modulo a prime, J. Number Theory 102(2003), 41-89.

[S6] Z.H. Sun, Quartic residues and binary quadratic forms, J. Number Theory 113(2005), 10-52.

[S7] Z.H. Sun, On the number of incongruent residues of x^4+ax^2+bx modulo p, J. Number Theory 119(2006), 210-241.

[S8] Z.H. Sun, Cubic residues and binary quadratic forms, J. Number Theory 124(2007), 62-104.

[S9] Z.H. Sun, On the quadratic character of quadratic units, J. Number Theory 128(2008), 1295-1335.

[S10] Z.H. Sun, Quartic, octic residues and Lucas sequences, J. Number Theory 129(2009), 499-550.

[S11] Z.H. Sun, Congruences for $(A+\sqrt{A^2+mB^2})^{\frac{p-1}{2}}$ and $(b+\sqrt{a^2+b^2})^{\frac{p-1}{4}} \pmod p$, Acta Arith. 149(2011), 275-296.

[S12] Z.H. Sun, Congruences for $q^{[p/8]} \pmod p$, Acta Arith. 159(2013), 1-25.

[S13] Z.H. Sun, On the quartic character of quadratic units, Acta Arith. 159(2013),89-100.

[S14] Z.H. Sun, New reciprocity laws for octic residues and nonresidues, J. Number Theory 147(2015), 694-707.

[S15] Z.H. Sun, Congruences for $q^{[p/8]} \pmod p$ under the condition $4n^2p = x^2 + qy^2$, Int. J. Number Theory 11(2015), 1301-1312.

[S16] Z.H. Sun, Quartic residues and sums involving $\binom{4k}{2k}$, Taiwanese J. Math. 19(2015),803-818.

[S17] Z.H. Sun, Cubic congruences and sums involving $\binom{3k}{k}$, Int. J. Number Theory 12(2016), 143-164.

§ 1. Rational cubic reciprocity law

Let $p > 3$ be a prime and $a \in \mathbb{Z}$ with $p \nmid a$. If $p \equiv 2 \pmod 3$, then $x^3 \equiv a \pmod p$ is always solvable.

If $p \equiv 1 \pmod 3$, Euler showed that there are unique positive integers L and M such that $4p = L^2 + 27M^2$.

Euler's Conjectures (1748-1750):

For any prime $p \equiv 1 \pmod 3$,

$$x^3 \equiv 2 \pmod p \text{ is solvable}$$
$$\iff p = A^2 + 27B^2 \ (A, B \in \mathbb{Z}),$$
$$x^3 \equiv 3 \pmod p \text{ is solvale}$$
$$\iff 4p = A^2 + 243B^2 \ (A, B \in \mathbb{Z}).$$

For any prime $p \equiv 1 \pmod 4$,

$$x^4 \equiv 2 \pmod p \text{ is solvable} \iff p = A^2 + 64B^2,$$
$$x^4 \equiv 5 \pmod p \text{ is solvable} \iff p = A^2 + 100B^2.$$

Let p be a prime of the form $3k+1$ and so $4p = L^2 + 27M^2$. For $a \in \mathbb{Z}$ with $p \nmid a$, since $(L/(3M))^2 \equiv -3 \pmod{p}$ we see that

$$x^3 \equiv a \pmod{p} \text{ is solvable } \iff a^{\frac{p-1}{3}} \equiv 1 \pmod{p},$$

and that

$$a^{\frac{p-1}{3}} \equiv 1, \frac{-1 + L/(3M)}{2} \text{ or } \frac{-1 - L/(3M)}{2} \pmod{p}.$$

Problem: Determine $a^{\frac{p-1}{3}} \pmod{p}$.

Jacobi(1827): Let p and q be distinct primes of the form $3k+1$, $4p = L^2 + 27M^2$, $4q = L'^2 + 27M'^2$. Then q is a cubic residue modulo p if and only if $(LM' - L'M)/(LM' + L'M)$ is a cubic residue modulo q.

Z.H. Sun([S2, 1998]): for $i = 0, 1, 2$,

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

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

Jacobi: $q^{\frac{p-1}{3}} \pmod{p}$ depends only on $\frac{L}{M} \pmod{q}$.

Let p be a prime of $4k+1$ and $4p = L^2 + 27M^2$. Then

$x^3 \equiv 5 \pmod{p}$ is solvable $\iff 5 \mid L$ or $5 \mid M$,

$x^3 \equiv 7 \pmod{p}$ is solvable $\iff 7 \mid L$ or $7 \mid M$,

$x^3 \equiv 11 \pmod{p}$ is solvable $\iff 11 \mid L,\ 11 \mid M$
or $L \equiv \pm 5 \cdot 3M \pmod{11}$,

$x^3 \equiv 13 \pmod{p}$ is solvable $\iff 13 \mid L,\ 13 \mid M$,
or $L \equiv \pm 4 \cdot 3M \pmod{13}$.

E. Lehmer (1959/1961): If $L \equiv M \pmod 4$, then

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

In 1975 K.S. Williams found a method to determine the sign of M such that $q^{\frac{p-1}{3}} \equiv \frac{-1-L/(3M)}{2} \pmod p$ when q is a cubic non-residue of p.

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

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

For $x, y \in C(q)$, in [S2] the author introduced the operation

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

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

Example:(1) $C(5) = \{0, \pm 1, \pm 2, \infty\}$.

$$1 * 2 = \frac{1 \cdot 2 - 3}{1 + 2} = -\frac{1}{3} = -2$$
$$1 * (-2) = \frac{1 \cdot (-2) - 3}{1 + (-2)} = 5 = 0.$$

(2) $C(7) = \{0, \pm 1, \pm 3, \infty\}$.

$$3 * 3 = \frac{3 \cdot 3 - 3}{3 + 3} = 1,$$
$$1 * (-1) = \frac{1 \cdot (-1) - 3}{1 + (-1)} = \infty.$$

Combining [S2, Corollary 2.1] with [S2, Theorem 3.2 and Corollary 3.3] we have:

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

q is a cubic residue modulo p

$$\iff \frac{L}{3M} \text{ is a cube in } C(q)$$

$$\iff q \mid M \text{ or } \frac{L}{3M} \equiv \frac{x^3 - 9x}{3x^2 - 3} \pmod q \text{ for some } x \in \mathbb{Z}.$$

For given prime $p > 3$ let $C_0(p)$ be the set of all cubes in $C(p)$. Suppose $s \in \{1, 2, \ldots, \frac{p-1}{2}\}$ and $s^2 \equiv -3 \pmod p$. Computing $\frac{x^3-9x}{3x^2-3} \pmod p$ for $x \in \{0, \pm 1, \pm 2, \ldots, \pm\frac{p-1}{2}\} - \{\pm s\}$ we get $C_0(p)$.

Example: $C_0(13) = \{0, \infty, \pm 4\}$. Thus,

13 is a cubic residue of p

$$\iff 13 \mid L,\ 13 \mid M \text{ or } \frac{L}{3M} \equiv \pm 4 \pmod{13}.$$

§2. The cubic Jacobi symbol

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

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

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

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

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

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

According to [IR, pp. 112-115, 135, 313] and [S2] the cubic Jacobi symbol has the following properties:

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

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

(2.2) (cubic reciprocity law (Eisenstein,1844; Jacobi,1837)) If $\pi, \lambda \in \mathbb{Z}[\omega]$ and $\pi, \lambda \equiv \pm 2 \pmod 3$, then

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

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

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

(2.4) If $m, n \in \mathbb{Z}$, $3 \nmid m$ and m is coprime to n, then $\left(\frac{n}{m}\right)_4 = 1$.

(2.5) If $\pi, \alpha, \beta \in \mathbb{Z}[\omega]$ and $\pi \equiv \pm 2 \pmod 3$, then $\left(\frac{\alpha\beta}{\pi}\right)_3 = \left(\frac{\alpha}{\pi}\right)_3 \left(\frac{\beta}{\pi}\right)_4$.

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

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

For a given prime p and $k \in \mathbb{F}_p$, we have

$$k \in C_0(p) \iff \left(\frac{k+1+2\omega}{p}\right)_3 = 1$$
$$\iff k \equiv \frac{x^3 - 9x}{3x^2 - 3} \pmod q \text{ for some } x \in \mathbb{Z}.$$

§3. The criterion for $m^{\frac{p-1}{3}} \pmod p$ in terms of binary quadratic forms

Theorem 3.1 ([S8, 2007]). *Let $p \equiv 1 \pmod 3$ be a prime. Let m be a cubefree integer with $m \not\equiv 0, \pm 1 \pmod p$ and $m \not\equiv 1 \pmod 3$. Let m_0 be the product of all distinct primes q satisfying $q \mid m$ and $q > 3$. Let k_3 be given by*

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

and $k = \frac{3+(-1)^m}{2} k_3 m_0$. Suppose $p = ax^2 + bxy + cy^2$ with $a, b, c, x, y \in \mathbb{Z}$, $b^2 - 4ac = -3k^2$ and $(a, 6m) = 1$. If $p \nmid a$, then

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

If $p \mid a$, then

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

Example: Let p be a prime of the form $3n+1$. Then

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

and

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

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

Let $d > 1$ be a squarefree integer, and let ε_d be the fundamental unit of the quadratic field $\mathbb{Q}(\sqrt{d})$. Then $\varepsilon_d = (m+n\sqrt{d})/2$ for some $m, n \in \mathbb{N}$ and $m^2 - dn^2 = \pm 4$. Let $p \equiv 1 \pmod 3$ be a prime such that $(\frac{d}{p}) = 1$. If $d \in \{2, 3, 5\}$, in 1973 E. Lehmer proved that ε_d is a cubic residue modulo p if and only if $p = x^2 + 27dy^2$ for some $x, y \in \mathbb{Z}$. In [S2], the author gave the criteria for ε_d to be a cubic residue of p in the cases $d = 6, 15, 21$.

Theorem 4.1. *Suppose* $m, n, d \in \mathbb{Z}$ *and* $m^2 - dn^2 = -4$. *Let* $p > 3$ *be a prime not dividing* d. *Let*

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

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

$$\left(\frac{m + n\sqrt{d}}{2}\right)^{\frac{p-(\frac{p}{3})}{3}}$$

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

If $p \mid a$, then

$$\left(\frac{m+n\sqrt{d}}{2}\right)^{\frac{p-(\frac{p}{3})}{3}}$$

$$\equiv \begin{cases} (\frac{p}{3}) \pmod{p} \\ \quad \text{if } \left(\frac{bn-km(1+2\omega)}{p}\right)_4 = 1, \\ \frac{1}{2}\left(-(\frac{p}{3}) + \frac{b\sqrt{d}}{kd}\right) \pmod{p} \\ \quad \text{if } \left(\frac{bn-km(1+2\omega)}{p}\right)_4 = \omega, \\ \frac{1}{2}\left(-(\frac{p}{3}) - \frac{b\sqrt{d}}{kd}\right) \pmod{p} \\ \quad \text{if } \left(\frac{bn-km(1+2\omega)}{p}\right)_4 = \omega^2. \end{cases}$$

Example 4.1 Let p be a prime such that $p \equiv 1, 5, 7, 11 \pmod{24}$. Then

$$
\begin{aligned}
&(1+\sqrt{2})^{\frac{p-1}{3}} \\
&\equiv \begin{cases} 1 \pmod{p} \quad \text{if } p = x^2 + 54y^2, \\ -\dfrac{1}{2} - \dfrac{7x+3y}{12y}\sqrt{2} \pmod{p} \\ \qquad \text{if } p = 7x^2 + 6xy + 9y^2 \neq 7, \end{cases} \\
&(1+\sqrt{2})^{\frac{p+1}{3}} \\
&\equiv \begin{cases} -1 \pmod{p} \quad \text{if } p = 2x^2 + 27y^2, \\ \dfrac{1}{2} + \dfrac{5x+y}{12y}\sqrt{2} \pmod{p} \\ \qquad \text{if } p = 5x^2 + 2xy + 11y^2 \neq 5. \end{cases}
\end{aligned}
$$

Example 4.2 Let $p > 3$ be a prime such that $(\frac{p}{17}) = (\frac{p}{3})$. Then

$$(4+\sqrt{17})^{\frac{p-1}{3}}$$
$$\equiv \begin{cases} 1 \pmod{p} \quad \text{if } p = x^2+xy+115y^2, \\ -\dfrac{1}{2} + \dfrac{26x+3y}{102y}\sqrt{17} \pmod{p} \\ \qquad\qquad \text{if } p = 13x^2+3xy+9y^2 \neq 13, \end{cases}$$
$$(4+\sqrt{17})^{\frac{p+1}{3}}$$
$$\equiv \begin{cases} -1 \pmod{p} \quad \text{if } p = 11x^2+5xy+11y^2, \\ \dfrac{1}{2} - \dfrac{10x+y}{102y}\sqrt{17} \pmod{p} \\ \qquad\qquad \text{if } p = 5x^2+xy+23y^2 \neq 5. \end{cases}$$

Theorem 4.2. *Suppose* $m, n, d \in \mathbb{Z}$, $m^2 - dn^2 = 4$ *and* $\mathrm{ord}_3(m-2) \geq \mathrm{ord}_3 n$. *Let* $p > 3$ *be a prime such that* $p \nmid dn$. *Let* $2^\alpha \parallel \frac{4(m-2)}{(m-2,n)^2}$. *Let*

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

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

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

If $p \nmid a$, then

$$\left(\frac{m+n\sqrt{d}}{2}\right)^{\frac{p-(\frac{p}{3})}{3}}$$

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

If $p \mid a$, then

$$\left(\frac{m+n\sqrt{d}}{2}\right)^{\frac{p-(\frac{p}{3})}{3}}$$

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

Example 4.3 If p is a prime such that $p \equiv 1 \pmod 3$ and $(\frac{7}{p}) = 1$, then

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

§5. **The criterion for** $p \mid U_{(p-(\frac{p}{3}))/3}(P,Q)$

The Lucas sequences $U_n(P,Q)$ and $V_n(P,Q)$ are given by

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

and

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

It is well known that

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

and

$$V_n(P,Q) = \left(\frac{P+\sqrt{D}}{2}\right)^n + \left(\frac{P-\sqrt{D}}{2}\right)^n,$$

where $D = P^2 - 4Q$.

For $a, b, c \in \mathbb{Z}$, $ax^2 + bxy + cy^2$ is called a binary quadratic form with **discriminant** $d = b^2 - 4ac$. If $\gcd(a, b, c) = 1$, we say that the form $ax^2 + bxy + cy^2$ is **primitive**. Denote the equivalence class containing the form $ax^2 + bxy + cy^2$ by $[a, b, c]$. Let $H(d)$ be the form class group consisting of classes of primitive, integral binary quadratic forms of discriminant d, and $h(d) = |H(d)|$. If $n \in \mathbb{N}$ is represented by one form in the class $[a, b, c]$, then n can be represented by any form in $[a, b, c]$ and we say that n is represented by $[a, b, c]$.

Problem: Determine all primes p so that $p \mid U_{(p-(\frac{p}{3}))/3}(P, Q)$.

Let $F_n = U_n(1, -1)$ be the Fibonacci sequence. For any prime $p > 3$ we have ([S2, 1998]):

$$p \mid F_{(p-(\frac{p}{3}))/3} \iff p = x^2 + 135y^2 \text{ or } 5x^2 + 27y^2,$$
$$p \mid F_{(p-(\frac{p}{3}))/6} \iff p = x^2 + 540y^2 \text{ or } 5x^2 + 108y^2.$$

Theorem 5.1 ([S8, 2007]). *Let $p > 3$ be a prime, and $P, Q \in \mathbb{Z}$ with $p \nmid PQ(P^2 - 4Q)$. Let $P^2 - 4Q = df^2$ $(d, f \in \mathbb{Z})$, $k = k(P/(P,f), f/(P,f), d)$ and*

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

(i) *$M(P,Q,f)$ is a subgroup of index 3 in $H(-3k^2d)$.*

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

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

Example 5.1 ([S8]): Let $p > 3$ be a prime. Then

$$p \mid U_{\frac{p-1}{3}}(3,-1) \iff p = x^2 + 351y^2, 13x^2 + 27y^2,$$
$$p \mid U_{\frac{p+1}{3}}(3,-1) \iff p = 11x^2 + 2xy + 32y^2.$$

§6. Cubic congruences and binary quadratic forms

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

(6.1)

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

It is known that D is the discriminant of $x^3 + a_1x^2 + a_2x + a_3$ and

(6.2)

$$N_p(x^3+a_1x^2+a_2x+a_3) = N_p(x^3-3Qx-PQ)\ (p \nmid Q).$$

It is well known that (Dickson, 1906; Skolem, 1952; Sun, 2003)

(6.3)

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

Theorem 6.1 ([S8, 2007]). *Let $p>3$ be a prime and $a_1,a_2,a_3\in\mathbb{Z}$. Let P and Q be given by* (6.1)*. Suppose $p\nmid PQ(P^2-4Q)$ and $P^2-4Q=df^2$ $(d,f\in\mathbb{Z})$. Then the congruence $x^3+a_1x^2+a_2x+a_3\equiv 0 \pmod p$ has three solutions if and only if p is represented by some class in $M(P,Q,f)$, where $M(P,Q,f)$ is a subgroup of $H(-3k^2d)$ given as in Theorem* 5.1*.*

Example 6.1. For prime $p>5$,

$$N_p(x^3-3x-10)=3 \iff p=x^2+162y^2, 2x^2+81y^2.$$

Theorem 6.2 (Spearman and Williams, 2001) Let $a_1, a_2, a_3 \in \mathbb{Z}$ be such that $f(x) = x^3 + a_1x^2 + a_2x + a_3$ is irreducible in $\mathbb{Z}[x]$. Let D be the discriminant of $f(x)$, and let d be the discriminant of the cubic field $\mathbb{Q}(t)$, where t is a root of $f(x) = 0$. Then there is a unique subgroup $J(a_1, a_2, a_3)$ of index 3 in $H(d)$ such that if $p > 3$ is a prime with $(\frac{D}{p}) = 1$, then the congruence $f(x) \equiv 0 \pmod{p}$ has three solutions if and only if p is represented by one of the classes in $J(a_1, a_2, a_3)$.

Let us compare Theorem 6.1 with Theorem 6.2. First Spearman and Williams proved Theorem 6.2 using class field theory, and we prove Theorem 6.1 using the theory of cubic residues. Second, the subgroup $M(P, Q, f)$ in Theorem 6.1 is constructed, but Spearman and Williams only proved the existence of the subgroup $J(a_1, a_2, a_3)$. Third, in some special cases, the discriminant of corresponding quadratic forms in Theorem 6.2 seems better than the discriminant in Theorem 6.1.

Dedekind(1899-1990): Let m be a cubefree integer. Then there is a subgroup H of index 3 in $H(-27m^2)$ with the property that m is a cubic residue modulo a prime $p \equiv 1 \pmod 3$ if and only if p is represented by a class in H.

Theorems 6.1 and 6.2 can be viewed as generalizations of Dedekind's result.

§7. **Quartic residues and binary quadratic forms**

Theorem 7.1 ([S6]) Suppose that m' is the product of all the distinct odd prime divisors of $m \in \mathbb{Z}$, $m = 2^{\alpha} m_0 (2 \nmid m_0)$ and $m^* = 4m'/(4, m_0 - \alpha - 1)$. If $p \equiv 1 \pmod 4$ is a prime such that $p \nmid m$, then m is a quartic residue (mod p) if and only if p is represented by one class in the set

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

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

Example 7.1 For prime $p \equiv 1 \pmod 4$ with $p \neq 5$,

5 is a quartic residue of $p \iff p = x^2 + 100y^2$,

-5 is a quartic residue of p
$\iff p = x^2 + 400y^2, 16x^2 + 16xy + 29y^2$.

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

When the norm $N(\varepsilon_d) = (m^2 - dn^2)/4 = -1$, many mathematicians tried to characterize those primes p ($p \equiv 1 \pmod 4$, $(\frac{d}{p}) = 1$) for which ε_d is a quadratic residue (mod p). In 1942 Aigner and Reichardt proved that $\varepsilon_2 = 1 + \sqrt{2}$ is a quadratic residue of a prime $p \equiv 1 \pmod 8$ if and only if $p = x^2 + 32y^2 (x, y \in \mathbb{Z})$. In 1969, Barrucand and Cohn rediscovered this result. Later, Brandler (1973) showed that for $q = 5, 13, 37$ the unit ε_q is a quadratic residue of a prime p ($p \equiv 1 \pmod 4$, $(\frac{q}{p}) = 1$) if and only if $p = x^2 + 4qy^2 (x, y \in \mathbb{Z})$. For more special results along this line one may consult [Lem, pp.168-170] (F. Lemmermeyer, Reciprocity Laws: From Euler to Eisenstein Springer, Berlin, 2000).

Theorem 7.2 ([S6, 2005]) Suppose that $p \equiv 1 \pmod 4$ is a prime, $d, m, n \in \mathbb{Z}$, $m^2 - dn^2 = -4$ and $(\frac{d}{p}) = 1$. Then $(m + n\sqrt{d})/2$ is a quadratic residue (mod p) if and only if p is represented by one class in the set

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

where

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

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

Example 7.2: Let p be a prime such that $(\frac{10}{p}) = 1$. Then $\varepsilon_{10} = 3 + \sqrt{10}$ is a quadratic residue of p if and only if p is represented by $x^2 + 160y^2$ or $13x^2 + 6xy + 13y^2$.

In [S9, 2008], using elementary arguments Z.H. Sun proved the following general result.

Theorem 7.3. *Let $p \equiv 1 \pmod 4$ be a prime and $p = c^2 + d^2$ with $c, d \in \mathbb{Z}$ and $2 \nmid c$. Suppose $a, b \in \mathbb{Z}$ with $(a, b) = 1$ and $p \nmid a(a^2 + b^2)$. Let*

$$\delta = \begin{cases} (\dfrac{bc+ad}{a^2+b^2}) & \text{if } 2 \mid a, \\ (-1)^{\frac{d}{2}}(\dfrac{ac-bd}{a^2+b^2}) & \text{if } 2 \mid b, \\ (-1)^{\frac{(bc+ad)^2-1}{8}}(\dfrac{bc+ad}{(a^2+b^2)/2}) & \text{if } 2 \nmid ab. \end{cases}$$

(i) *If* $(\frac{a^2+b^2}{p}) = 1$, *then*

$$\left(\frac{(b+\sqrt{a^2+b^2})/2}{p}\right) \equiv \delta \pmod p.$$

(ii) *If* $(\frac{a^2+b^2}{p}) = -1$, *then*

$$\left(\frac{b+\sqrt{a^2+b^2}}{2}\right)^{\frac{p-1}{2}} \equiv \delta\frac{b-\sqrt{a^2+b^2}}{a} \pmod p.$$

Example 7.3: Suppose that $p \equiv 1 \pmod 4$ is a prime and $p = c^2 + d^2$ with $2 \mid d$. Then

$$\Big(\frac{1+\sqrt{5}}{2}\Big)^{\frac{p-1}{2}} \equiv \begin{cases} (\frac{c+2d}{5}) \pmod p \\ \quad \text{if } p \equiv 1, 9 \pmod{20}, \\ (\frac{c+2d}{5})\frac{c}{d} \cdot \frac{1-\sqrt{5}}{2} \pmod p \\ \quad \text{if } p \equiv 13, 17 \pmod{20}. \end{cases}$$

In 1974, using the cyclotomic numbers of order 12, E. Lehmer proved that $\varepsilon_3 = 2 + \sqrt{3}$ is a quartic residue of a prime $p \equiv 1 \pmod{12}$ if and only if $p = x^2 + 192y^2$ for some integers x and y. She also conjectured that $\varepsilon_7 = 8 + 3\sqrt{7}$ is a quartic residue of p if and only if $p = x^2 + 448y^2$ for some integers x and y. In 1977, P.A. Leonard and K.S. Williams proved Lehmer's conjecture and gave some additional special results. They barely obtained partial results in the cases $d = 3, 7, 11, 19, 43, 67, 163, 6, 14, 22, 38, 86, 134$. In [S6] we completely solved the problem by proving the following general result.

Theorem 7.4 Suppose that $p \equiv 1 \pmod 4$ is a prime, $m, n, d \in \mathbb{Z}$, $m^2 - dn^2 = 4$, $p \nmid n$ and $(\frac{d}{p}) = 1$. Then $(m + n\sqrt{d})/2$ is a quartic residue (mod p) if and only if p is represented by one class in the set

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

where $\delta(n,d) \in \{1,2,4,8\}$ is explicitly given by [S6,Table 4]. Moreover, $N_0(m,n,d)$ is a subgroup of $H(-4\delta(n,d)^2 d)$.

Example 7.4: Let p be an odd prime such that $(\frac{15}{p}) = 1$. Then $\varepsilon_{15} = 4 + \sqrt{15}$ is a quartic residue of p if and only if $p = x^2 + 960y^2$ or $20x^2 + 20xy + 53y^2$.

Let p be an odd prime such that $(\frac{Q}{p}) = (\frac{4Q-P^2}{p}) = 1$. It is well known that $p \mid U_{(p-(\frac{-1}{p}))/4}(P,Q)$ or $p \mid V_{(p-(\frac{-1}{p}))/4}(P,Q)$. How to characterize those odd primes p so that $p \mid U_{(p-(\frac{-1}{p}))/4}(P,Q)$? Suppose that $p \equiv 1 \pmod 4$ $(p \neq 5)$ is a prime and that $\{F_n\}$ $(F_n = U_n(1,-1))$ is the Fibonacci sequence. In 1992 Z.H. Sun and Z.W. Sun showed that $p \mid F_{\frac{p-1}{4}}$ if and only if $p = x^2 + 80y^2$ or $16x^2 + 5y^2$ with $x, y \in \mathbb{Z}$. Let $P_n = U_n(2,-1)$ be the Pell sequence. In 1974 E. Lehmer showed that $p \mid P_{\frac{p-1}{4}}$ if and only if $p = x^2 + 32y^2$ for some $x, y \in \mathbb{Z}$.

Theorem 7.5 Let p be an odd prime, $P, Q \in \mathbb{Z}$, $p \nmid Q(P^2 - 4Q)$, and let Q' be the product of all distinct odd prime divisors of Q. If $Q = 2^t Q_0 (2 \nmid Q_0)$,

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

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

$$G(P,Q) = \Big\{ [a,2b,c] \;\Big|\; [a,2b,c] \in H(-4k^2(P^2-4Q)), \\ (a,2Q) = 1,\ \Big(\frac{kP+bi}{a}\Big)_4 = 1 \Big\}.$$

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

§8. **Cubic and quartic congruences modulo a prime**

For integers a_1, a_2, a_3 let $\{s_n\}$ be the third-order recurring sequence defined by

$$s_0 = 3,\ s_1 = -a_1,\ s_2 = a_1^2 - 2a_2,$$
$$s_{n+3} + a_1 s_{n+2} + a_2 s_{n+1} + a_3 s_n = 0\ (n \ge 0).$$

If $x^3+a_1x^2+a_2x+a_3 = (x-x_1)(x-x_2)(x-x_3)$, then $s_n = x_1^n + x_2^n + x_3^n$.

Theorem 8.1 ([S5, 2003]) Let $p > 3$ be a prime, and $a_1, a_2, a_3 \in \mathbb{Z}$. If $p \nmid a_1^2 - 3a_2$, we have

$$N_p(x^3 + a_1x^2 + a_2x + a_3)$$
$$= \begin{cases} 3 & \text{if } s_{p+1} \equiv a_1^2 - 2a_2 \pmod p, \\ 0 & \text{if } s_{p+1} \equiv a_2 \pmod p, \\ 1 & \text{if } s_{p+1} \not\equiv a_2, a_1^2 - 2a_2 \pmod p. \end{cases}$$

Moreover, if $N_p(x^3+a_1x^2+a_2x+a_3) = 1$, then the unique solution of the congruence $x^3 + a_1x^2 + a_2x + a_3 \equiv 0 \pmod{p}$ is given by

$$x \equiv \frac{2a_1a_2 - 9a_3 - a_1s_{p+1}}{-2a_1^2 + 3a_2 + 3s_{p+1}} \pmod{p};$$

if $N_p(x^3+a_1x^2+a_2x+a_3) = 0$ and $p \nmid a_1^2 - 3a_2$, then $(2s_{p+2} + a_1a_2 - 3a_3)^2 \equiv D \pmod{p}$; if $N_p(x^3 + a_1x^2 + a_2x + a_3) = 3$, $p \nmid D$ and $x_0 = \frac{1}{2}((\frac{-a_3}{p})s_{\frac{p+1}{2}} - a_1) \not\equiv -a_1 \pmod{p}$, then

$$x \equiv x_0,\ \frac{1}{2}(-a_1 - x_0 \pm \frac{d}{3x_0^2 + 2a_1x_0 + a_2}) \pmod{p}$$

are the three solutions of the congruence $x^3 + a_1x^2 + a_2x + a_3 \equiv 0 \pmod{p}$, where d is an integer such that $d^2 \equiv D \pmod{p}$.

For integers a_1, a_2, a_3 let $\{u_n\}$ be the third-order recurring sequence defined by

$$u_{-2} = u_{-1} = 0,\ u_0 = 1,$$
$$u_{n+3} + a_1u_{n+2} + a_2u_{n+1} + a_3u_n = 0 \ (n \geq -2).$$

Theorem 8.2 ([S5,2003]) Let $p > 3$ be a prime and $a_1, a_2, a_3 \in \mathbb{Z}_p$. Suppose $P = -2a_1^3 + 9a_1a_2 - 27a_3$, $Q = (a_1^2 - 3a_2)^3$ and $D = -(P^2 - 4Q)/27$ and $PQ \not\equiv 0 \pmod p$. Then

$$N_p(x^3 + a_1x^2 + a_2x + a_3)$$
$$= \begin{cases} 3 & \text{if } Du_{p-2}^2 \equiv 0 \pmod p, \\ 0 & \text{if } Du_{p-2}^2 \equiv (a_1^2 - 3a_2)^2 \pmod p, \\ 1 & \text{if } Du_{p-2}^2 \not\equiv 0, (a_1^2 - 3a_2)^2 \pmod p. \end{cases}$$

Theorem 8.3 ([S17,2016]) Let $p > 3$ be a prime and $a_1, a_2, a_3 \in \mathbb{Z}_p$. Suppose $P = -2a_1^3 + 9a_1a_2 - 27a_3$, $Q = (a_1^2 - 3a_2)^3$ and $PQ(P^2 - 4Q) \not\equiv 0 \pmod p$. Then $N_p(x^3 + a_1x^2 + a_2x + a_3) = 1$ if and only if

$$x \equiv \frac{P}{3(a_1^2 - 3a_2)} \sum_{k=0}^{[p/3]} \binom{3k}{k} \left(\frac{4Q - P^2}{27Q}\right)^k - \frac{a_1}{3} \pmod p$$

is a solution of the congruence $x^3 + a_1x^2 + a_2x + a_3 \equiv 0 \pmod p$. If $P^2 \not\equiv Q, 3Q \pmod p$, then $N_p(x^3 + a_1x^2 + a_2x + a_3) = 3$ if and only if $\sum_{k=1}^{[p/3]} \binom{3k}{k} (\frac{4Q-P^2}{27Q})^k \equiv 0 \pmod p$.

Theorem 8.4 ([S5, 2003]) Let $p > 3$ be a prime, $a, b, c \in \mathbb{Z}$, and let $\{S_n\}$ be given by

$$S_0 = 3,\ S_1 = -2a,\ S_2 = 2a^2 + 8c,$$
$$S_{n+3} = -2aS_{n+2} + (4c - a^2)S_{n+1} + b^2 S_n\ (n \geq 0).$$

If $p \nmid a^2 + 12c$, then

$$N_p(x^4 + ax^2 + bx + c) = 1$$
$$\iff S_{p+1} \equiv a^2 - 4c \pmod{p}.$$

If $N_p(x^4 + ax^2 + bx + c) = 1$, then the unique solution of the congruence $x^4 + ax^2 + bx + c \equiv 0 \pmod{p}$ is given by

$$x \equiv \frac{a^2 - 4c - S_{\frac{p+1}{2}}^2}{4b} \pmod{p}.$$

Theorem 8.5 Let $p > 3$ be a prime, $a, b, c \in \mathbb{Z}$, $D(a,b,c) = -(4a^3 + 27b^2)b^2 + 16c(a^4 + 9ab^2 - 8a^2c + 16c^2)$ and $p \nmid bD(a,b,c)$. Then $N_p(x^4 + ax^2 + bx + c) = 0$ if and only if there exists an integer y such that $y^3 + 2ay^2 + (a^2 - 4c)y - b^2 \equiv 0 \pmod{p}$ and $(\frac{y}{p}) = -1$. When $N_p(x^4 + ax^2 + bx + c) > 0$ we have

$$\begin{aligned} &N_p(x^4 + ax^2 + bx + c) \\ &= N_p(y^3 + 2ay^2 + (a^2 - 4c)y - b^2) + 1. \end{aligned}$$

(T. Skolem, 1952; Z.H. Sun, 2003)

§9. **Conjectures for** $U_{(p-(\frac{-1}{p}))/4}(P,Q) \pmod p$ **and** $q^{[p/8]} \pmod p$

In 1980 and 1984 Hudson and Williams proved the following result.

Theorem 9.1. *Let* $p \equiv 1 \pmod{24}$ *be a prime and hence* $p = c^2 + d^2 = x^2 + 3y^2$ *for some* $c, d, x, y \in \mathbb{Z}$. *Suppose* $c \equiv 1 \pmod 4$.

(i) ([HW1]) *If* $c \equiv \pm(-1)^{\frac{y}{4}} \pmod 3$, *then* $3^{\frac{p-1}{8}} \equiv \pm 1 \pmod p$.

(ii) ([H]) *If* $d \equiv \pm(-1)^{\frac{y}{4}} \pmod 3$, *then* $3^{\frac{p-1}{8}} \equiv \pm\frac{d}{c} \pmod p$.

Hudson and Williams proved Theorem 9.1(i) by using the cyclotomic numbers of order 12, and Hudson proved Theorem 9.1(ii) using the Jacobi sums of order 24.

Now we pose some conjectures similar to Theorem 9.1.

Conjecture 9.1. *Let* $p \equiv 1 \pmod 4$ *and* $q \equiv 3 \pmod 8$ *be primes such that* $p = c^2 + d^2 = x^2 + qy^2$ *with* $c, d, x, y \in \mathbb{Z}$ *and* $q \mid cd$. *Suppose* $c \equiv x \equiv 1 \pmod 4$, $y = 2^\beta y_0$ *and* $y_0 \equiv 1 \pmod 4$.

(i) *If* $p \equiv 1 \pmod 8$, *then*

$$q^{\frac{p-1}{8}} \equiv \begin{cases} \pm(-1)^{\frac{y}{4}} \pmod p & \text{if } x \equiv \pm c \pmod q, \\ \mp(-1)^{\frac{q-3}{8}+\frac{y}{4}} \dfrac{d}{c} \pmod p & \text{if } x \equiv \pm d \pmod q. \end{cases}$$

(ii) *If* $p \equiv 5 \pmod 8$, *then*

$$q^{\frac{p-5}{8}} \equiv \begin{cases} \pm\dfrac{y}{x} \pmod p & \text{if } x \equiv \pm c \pmod q, \\ \mp(-1)^{\frac{q-3}{8}} \dfrac{dy}{cx} \pmod p & \text{if } x \equiv \pm d \pmod q. \end{cases}$$

Conjecture 9.2. *Let* $p \equiv 1 \pmod 4$ *and* $q \equiv 7 \pmod{16}$ *be primes such that* $p = c^2 + d^2 = x^2 + qy^2$ *with* $c, d, x, y \in \mathbb{Z}$ *and* $q \mid cd$. *Suppose* $c \equiv x \equiv 1 \pmod 4$, $y = 2^\beta y_0$ *and* $y_0 \equiv 1 \pmod 4$.

(i) If $p \equiv 1 \pmod 8$, then

$$q^{\frac{p-1}{8}} \equiv \begin{cases} (-1)^{\frac{y}{4}} \pmod p & \text{if } q \mid d, \\ -(-1)^{\frac{y}{4}} \pmod p & \text{if } q \mid c. \end{cases}$$

(ii) If $p \equiv 5 \pmod 8$, then

$$q^{\frac{p-5}{8}} \equiv \begin{cases} \dfrac{y}{x} \pmod p & \text{if } q \mid d, \\ -\dfrac{y}{x} \pmod p & \text{if } q \mid c. \end{cases}$$

Conjecture 9.3. *Let* $p \equiv 1 \pmod 4$ *and* $q \equiv 15 \pmod{16}$ *be primes such that* $p = c^2 + d^2 = x^2 + qy^2$ *with* $c, d, x, y \in \mathbb{Z}$ *and* $q \mid cd$. *Suppose* $y = 2^\beta y_0$ *and* $x \equiv y_0 \equiv 1 \pmod 4$.

(i) *If* $p \equiv 1 \pmod 8$, *then* $q^{\frac{p-1}{8}} \equiv (-1)^{\frac{y}{4}} \pmod p$.

(ii) *If* $p \equiv 5 \pmod 8$, *then* $q^{\frac{p-5}{8}} \equiv \frac{y}{x} \pmod p$.

In [S12] Z.H. Sun proved Conjectures 9.1-9.3 on condition that $(c, x + d) = 1$ or $(d, x + c) = 2^s$.

Conjecture 9.4. *Let* $p \equiv 3 \pmod 8$ *be a prime and* $k \in \mathbb{Z}$ *with* $2 \nmid k$. *Suppose* $p = x^2 + (k^2+1)y^2$ *for some* $x, y \in \mathbb{Z}$. *Then*

$$V_{\frac{p+1}{4}}(2k,-1) \equiv \begin{cases} -(-1)^{\frac{(\frac{p-1}{2}y)^2-1}{8}} 2^{\frac{p+1}{4}} \pmod p \\ \qquad \textit{if } k \equiv 5,7 \pmod 8, \\ (-1)^{\frac{(\frac{p-1}{2}y)^2-1}{8}} 2^{\frac{p+1}{4}} \pmod p \\ \qquad \textit{if } k \equiv 1,3 \pmod 8. \end{cases}$$

In the case $k = 1$ Conjecture 4.1 was proved by the author in [S10,2009] and C.N. Beli (Acta Arith. 137(2009), 99-131).

Conjecture 9.5. *Let $p \equiv 3 \pmod 4$ be a prime and $k \in \mathbb{Z}$ with $2 \nmid k$. Suppose $2p = x^2 + (k^2+4)y^2$ for some $x, y \in \mathbb{Z}$.*

(i) *If $k \equiv 1, 3 \pmod 8$, then*

$$V_{\frac{p+1}{4}}(k, -1)$$
$$\equiv \begin{cases} (-1)^{\frac{(\frac{p-1}{2}y)^2-1}{8}}(-2)^{\frac{p+1}{4}} \pmod p \\ \qquad \text{if } k \equiv 1, 11 \pmod{16}, \\ -(-1)^{\frac{(\frac{p-1}{2}y)^2-1}{8}}(-2)^{\frac{p+1}{4}} \pmod p \\ \qquad \text{if } k \equiv 3, 9 \pmod{16}. \end{cases}$$

(ii) *If $k \equiv 5, 7 \pmod 8$, then*

$$V_{\frac{p+1}{4}}(k, -1) \equiv \begin{cases} (-1)^{\frac{(\frac{p-1}{2}y)^2-1}{8}}2^{\frac{p+1}{4}} \pmod p \\ \qquad \text{if } k \equiv 5, 15 \pmod{16}, \\ -(-1)^{\frac{(\frac{p-1}{2}y)^2-1}{8}}2^{\frac{p+1}{4}} \pmod p \\ \qquad \text{if } k \equiv 7, 13 \pmod{16}. \end{cases}$$

In the case $k = 1$ Conjecture 9.5 was proved by C.N. Beli in 2009.

Conjecture 9.6. *Let* $p \equiv 1 \pmod 4$ *be a prime,* $b \in \mathbb{Z}$, $2 \nmid b$ *and* $p = c^2 + d^2 = x^2 + (b^2 + 4)y^2 \neq b^2 + 4$ *for some* $c, d, x, y \in \mathbb{Z}$. *Suppose* $c \equiv 1 \pmod 4$ *and all the odd parts of* d, x, y *are numbers of the form* $4k + 1$.

(i) *If* $4 \nmid xy$, *then*

$$U_{\frac{p-1}{4}}(b, -1) \equiv \begin{cases} (-1)^{\frac{d}{4}} \dfrac{2y}{x} \pmod p \\ \qquad \text{if } 2 \parallel x \text{ and } b \equiv 1, 3 \pmod 8, \\ -(-1)^{\frac{d}{4}} \dfrac{2y}{x} \pmod p \\ \qquad \text{if } 2 \parallel x \text{ and } b \equiv 5, 7 \pmod 8, \\ \dfrac{2dy}{cx} \pmod p \\ \qquad \text{if } 2 \parallel y. \end{cases}$$

(ii) If $4 \mid xy$, then

$$V_{\frac{p-1}{4}}(b,-1) \equiv \begin{cases} 2(-1)^{\frac{d+y}{4}} \pmod p & \text{i} \\ -2(-1)^{\frac{x}{4}}\frac{d}{c} \pmod p \\ \qquad \text{if } 4 \mid x \text{ and } b \equiv 1,3 \pmod 8. \\ 2(-1)^{\frac{x}{4}}\frac{d}{c} \pmod p \\ \qquad \text{if } 4 \mid x \text{ and } b \equiv 5,7 \pmod 8. \end{cases}$$

Conjecture 9.6 has been checked for $b < 60$ and $p < 20000$. When $p \equiv 1 \pmod 8$, $b = 1,3$ and $4 \mid y$, the conjecture $V_{\frac{p-1}{4}}(b,-1) \equiv 2(-1)^{\frac{d+y}{4}} \pmod p$ is equivalent to a conjecture of E. Lehmer.

In [S13] Z.H. Sun proved Conjecture 9.6 on condition that $(c, x+d) = 1$ or $(d, x+c) = 2^s$.

Conjecture 9.7. *Let $a \in \mathbb{Z}$, $a \neq 0$ and let $p \equiv 1 \pmod 4$ be a prime such that $p = c^2 + d^2 = x^2 + (4a^2+1)y^2$ with $c, d, x, y \in \mathbb{Z}$, $c \equiv 1 \pmod 4$ and $p \neq 4a^2 + 1$. Suppose $d = 2^r d_0$, $y = 2^t y_0$ and $d_0 \equiv y_0 \equiv 1 \pmod 4$.*

(i) If $p \equiv 1 \pmod 8$, then

$$U_{\frac{p-1}{4}}(4a,-1) \equiv \begin{cases} (-1)^{\frac{a+1}{2}+\frac{d}{4}+\frac{x-2}{4}}\overline{\frac{y}{x}} \pmod p \\ \qquad\qquad \text{if } 2 \nmid ay, \\ 0 \pmod p \quad \text{if } 2 \mid ay \end{cases}$$

and

$$V_{\frac{p-1}{4}}(4a,-1) \equiv \begin{cases} 2(-1)^{\frac{d}{4}+\frac{a}{2}y+\frac{xy}{4}} \pmod p \\ \qquad\qquad \text{if } 2 \mid a, \\ 2(-1)^{\frac{d}{4}+\frac{y}{4}} \pmod p \\ \qquad\qquad \text{if } 2 \nmid a \text{ and } 2 \mid y, \\ 0 \pmod p \quad \text{if } 2 \nmid ay. \end{cases}$$

(ii) If $p\equiv 5 \pmod 8$, then

$$U_{\frac{p-1}{4}}(4a,-1)\equiv\begin{cases}(-1)^{\frac{a}{2}+\frac{x-2}{4}}\dfrac{dy}{cx} \pmod p\\ \qquad \text{if } 2\mid a \text{ and } 2\nmid y,\\ (-1)^{\frac{x+1}{2}}\dfrac{dy}{cx} \pmod p\\ \quad \text{if } 2\mid a \text{ and } 2\mid y,\\ \dfrac{dy}{cx} \pmod p\\ \quad \text{if } 2\nmid a \text{ and } 2\mid y,\\ 0 \pmod p \quad \text{if } 2\nmid ay\end{cases}$$

and

$$V_{\frac{p-1}{4}}(4a,-1)\equiv\begin{cases}0 \pmod p \quad \text{if } 2\mid ay,\\ 2(-1)^{\frac{a-1}{2}+\frac{x}{4}}\dfrac{d}{c} \pmod p\\ \qquad \text{if } 2\nmid ay.\end{cases}$$

In [S13] Z.H. Sun proved Conjecture 9.7 on condition that $(c,x+d)=1$ or $(d,x+c)=2^s$.

Conjecture 9.8 ([S10]). *Let* $p \equiv 1 \pmod 4$ *be a prime,* $b \in \mathbb{Z}$, $b \equiv 2 \pmod 4$, $p \neq b^2/4+1$ *and* $p = c^2 + d^2 = x^2 + (1 + b^2/4)y^2$ *for some* $c, d, x, y \in \mathbb{Z}$. *Suppose* $c \equiv 1 \pmod 4$, $x = 2^\alpha x_0$, $y = 2^\beta y_0$ *and* $x_0 \equiv y_0 \equiv 1 \pmod 4$. *Then*

$$U_{\frac{p-1}{4}}(b,-1) \equiv \begin{cases} (-1)^{\frac{b-2}{4}+\frac{d}{4}}\dfrac{y}{x} \pmod p & \text{if } 2 \parallel y, \\ 0 \pmod p & \text{if } 4 \mid y \end{cases}$$

and

$$V_{\frac{p-1}{4}}(b,-1) \equiv \begin{cases} 0 \pmod p & \text{if } 2 \parallel y, \\ 2(-1)^{\frac{d}{4}+\frac{y}{4}} \pmod p & \text{if } 4 \mid y. \end{cases}$$

In [S14] Z.H. Sun proved Conjecture 9.8 on condition that $(c, x + d) = 1$ or $(d, x + c) = 2^s$.

§10. Evaluation of $V_p(x^4 + ax^2 + bx)$

For a positive integer m and given polynomial $f(x)$ with integral coefficients, denote the number of incongruent residues of $f(x)(x \in \mathbb{Z})$ modulo m by $V_m(f(x))$. That is,

$$V_m(f(x)) = \Big|\Big\{c \;\Big|\; c \in \{0, 1, \ldots, m-1\}, \; f(x) \equiv c \pmod{m} \text{ is solvable}\Big\}\Big|.$$

For any odd prime p we have $V_p(x^2) = \frac{p+1}{2}$.

Let $p > 3$ be a prime and $a_1, a_2, a_3 \in \mathbb{Z}$. In 1908 R.D. von Sterneck proved that if $a_1^2 \not\equiv 3a_2 \pmod{p}$, then

$$V_p(x^3 + a_1x^2 + a_2x + a_3) = \frac{2p + (\frac{p}{3})}{3}.$$

Theorem 10.1 ([S7]). *Let* $p \equiv 2 \pmod 3$ *be an odd prime,* $b \in \mathbb{Z}$ *and* $p \nmid b$. *Then*

$$V_p(x^4 + bx) = \left[\frac{5p+7}{8}\right].$$

Theorem 10.2 ([S7]). *Let* $p \equiv 1 \pmod 3$ *be a prime,* $p = A^2 + 3B^2 (A, B \in \mathbb{Z})$, $A \equiv 1 \pmod 3$, $b \in \mathbb{Z}$ *and* $p \nmid b$.

(i) *If* $p \equiv 1 \pmod{12}$, *then*

$$V_p(x^4+bx) = \begin{cases} \dfrac{1}{8}(5p + 9 - 6(-1)^{\frac{p-1}{12}}) \\ \quad \textit{if } 2b \textit{ is a cubic residue } (\mathrm{mod}\ p), \\ \dfrac{1}{8}(5p + 3 \pm 6B) \\ \quad \textit{if } (2b)^{\frac{p-1}{3}} \equiv \frac{1}{2}\Big(-1 \mp \frac{A}{B}\Big) \pmod p. \end{cases}$$

(ii) If $p \equiv 7 \pmod{12}$, then

$$V_p(x^4+bx) = \begin{cases} \frac{1}{8}(5p+7+6(-1)^{\frac{p-7}{12}}-4A) \\ \text{ if } 2b \text{ is a cubic residue (mod } p), \\ \frac{1}{8}(5p+1+2A) \\ \text{ if } 2b \text{ is a cubic nonresidue (mod } p). \end{cases}$$

Theorem 10.3 ([S7]). *Let p be a prime greater than* 3.

(i) *If $p \equiv 1 \pmod{12}$ and $p = A^2+3B^2 = c^2+d^2$ with $2 \mid d$, $c+d \equiv 1 \pmod 4$ and $A \equiv 1 \pmod 3$, then*

$$V_p(x^4-3x^2+2x) = \begin{cases} \frac{1}{8}(5p+3+4\delta(p)-2A-2c) & \text{if } 3 \mid c, \\ \frac{1}{8}(5p+3+4\delta(p)-2A+2c) & \text{if } 3 \mid d, \end{cases}$$

where

$$\delta(p) = \begin{cases} 1 & \text{if } p \equiv 13 \pmod{24}, \\ 0 & \text{if } p \equiv 1 \pmod{24} \text{ and } B \equiv d \pmod 8, \\ 2 & \text{if } p \equiv 1 \pmod{24} \text{ and } B \not\equiv d \pmod 8. \end{cases}$$

(ii) If $p \equiv 5 \pmod{12}$ and $p = c^2 + d^2$ with $2 \mid d$, $c + d \equiv 1 \pmod 4$ and $c \equiv d \pmod 3$, then

$$V_p(x^4 - 3x^2 + 2x) = \frac{1}{8}\Big(5p + 3 - 2d\Big).$$

(iii) If $p \equiv 7 \pmod{12}$ and $p = A^2 + 3B^2$ with $A \equiv 1 \pmod 3$, then

$$V_p(x^4 - 3x^2 + 2x) = \frac{1}{8}\Big(5p + 1 - 2A\Big).$$

(iv) If $p \equiv 11 \pmod{12}$, then

$$V_p(x^4 - 3x^2 + 2x)$$
$$= \begin{cases} \dfrac{5p+1}{8} + \dfrac{1}{2}\Big(1 - \big(\dfrac{3^{\frac{p+1}{4}} + 1}{p}\big)\Big) & \text{if } 24 \mid p - 11, \\ \dfrac{5}{8}(p+1) & \text{if } 24 \mid p - 23. \end{cases}$$

Theorem 10.4. *Let $p > 3$ be a prime, and $a, b \in \mathbb{Z}$ with $p \nmid b$. Then*

$$\left|V_p(x^4 + ax^2 + bx) - \frac{5p}{8}\right| \le \frac{1}{2}\sqrt{p} + \frac{15}{8}.$$