ON THE JACOBSTHAL SUM $\varphi_k(a)$ AND
THE RELATED SUM $\psi_k(a)$

S. A. KATRE and A. R. RAJWADE

1. Introduction.

For an odd prime $p$ and a positive integer $k$, the Jacobsthal sums $\varphi_k(a)$ and
the related sums $\psi_k(a)$, of order $k$, are defined by

$$\varphi_k(a) = \sum_{x=0}^{p-1} \left( \frac{x}{p} \right) \left( \frac{x^k + a}{p} \right)$$

and

$$\psi_k(a) = \sum_{x=0}^{p-1} \left( \frac{x^k + a}{p} \right),$$

where $\left( . / p \right)$ is the Legendre symbol and $a \in \mathbb{Z}$, the ring of rational integers. The
sums are easily obtained if $a \equiv 0 \pmod{p}$, and if $p \equiv 1 \pmod{k}$, they reduce to sums of lower order. These sums are related by

\[ (1.1) \quad \varphi_k(a) = \psi_{2k}(a) - \psi_k(a), \]

and if $k$ is odd and $a \not\equiv 0 \pmod{p}$ we also have

\[ (1.2) \quad \varphi_k(a) = -1 + (a/p)\psi_k(\bar{a}), \]

where $\bar{a}$ satisfies $a\bar{a} \equiv 1 \pmod{p}$. $\varphi_2(a)$ was first evaluated by Davenport and
Hasse [2] (1935), $\varphi_3(a)$ and $\varphi_5(a)$ were first evaluated by Rajwade [8] (1969),
[9] (1973), and $\varphi_k(a)$ for all odd primes $k < 23$ by Leonard and Williams [7]
(1978). In all these cases, the corresponding cyclotomic field (that is $\mathbb{Q}(\zeta_k)$ if $k$

is odd and $\mathbb{Q}(\zeta_{2k})$ if $k$ is even, where $\mathbb{Q}$ is the field of rational numbers and $\zeta_k$

$= \exp(2\pi i / k))$ is of class number 1, and for $p \equiv 1 \pmod{k}$, the result was

obtained in terms of suitable normalized prime factors of $p$ in this field.

As far as the prime power values of $k$ are concerned, the evaluation of $\varphi_4(a)$

has already been accomplished by the present authors [6]. In the present

paper, we shall evaluate $\varphi_9(a)$ and $\psi_9(a)$.

Received March 23, 1982.

Math. Scand. 53 — 13
2. Preliminaries.

In what follows (unless stated otherwise) let $p$ be a prime $\equiv 1 \pmod{9}$, $a$ an integer not divisible by $p$, $\zeta = \exp(2\pi i/9)$, and $\omega = \exp(2\pi i/3)$. Then $\zeta$ and $\omega$ satisfy the irreducible equations (over $\mathbb{Q}$) $\zeta^6 + \zeta^3 + 1 = 0$ and $\omega^2 + \omega + 1 = 0$, $\mathbb{Z}[\zeta]$ and $\mathbb{Z}[\omega]$ are PID’s, $1 - \zeta$ is a prime in $\mathbb{Z}[\zeta]$, and as ideals, $(3) = (1 - \zeta)^6$ and $(1 - \omega) = (1 - \zeta)^3$. Let $\sigma$ be the automorphism of $\mathbb{Q}(\zeta)$ over $\mathbb{Q}$ such that $\sigma(\zeta) = \zeta^2$. Then

$$\text{Gal}\left(\mathbb{Q}(\zeta)/\mathbb{Q}\right) = \{1, \sigma, \sigma^2, \sigma^3, \sigma^4, \sigma^5\}.$$ 

Let $\pi_0$ be any prime factor of $p$ in $\mathbb{Z}[\zeta]$. Then $p = \pi_0 \pi_1 \pi_2 \pi_3 \pi_4 \pi_5$, where $\pi_i = \sigma^i(\pi_0)$, $0 \leq i \leq 5$. For any prime factor $\pi$ of $p$ in $\mathbb{Z}[\zeta]$ and for $\alpha \in \mathbb{Z}[\zeta]$, we define the ninth power residue symbol $(\alpha/\pi)_9$ by $(\alpha/\pi)_9 = 0$, if $\alpha^{(p - 1)/9} \equiv 0$, $\zeta^i$ (mod $\pi$), $0 \leq i \leq 8$, and the eighteenth power residue symbol $(\alpha/\pi)_{18}$ by $(\alpha/\pi)_{18} = 0$, if $\alpha^{(p - 1)/18} \equiv 0$, $\pm \zeta^i$ (mod $\pi$), $0 \leq i \leq 8$. Similarly for a prime factor $\mu$ of $p$ in $\mathbb{Z}[\omega]$ and for $\alpha \in \mathbb{Z}[\omega]$ we define $(\alpha/\mu)_3 = 0, 1, \omega, \omega^2$ according as $\alpha^{(p - 1)/3} \equiv 0, 1, \omega, \omega^2$ (mod $\mu$) and $(\alpha/\mu)_6 = 0, 1, \pm 1, \pm \omega, \pm \omega^2$ according as $\alpha^{(p - 1)/6} \equiv 0, 1, \pm 1, \pm \omega, \pm \omega^2$ (mod $\mu$). For $b \in \mathbb{Z}$, one can easily prove that

$$\begin{align*}
(b/\lambda \pi)_k &= \lambda(b/\pi)_k, \quad \text{for } k = 9, 18, \lambda \in \text{Gal}\left(\mathbb{Q}(\zeta)/\mathbb{Q}\right), \\
(b/\lambda \mu)_k &= \lambda(b/\mu)_k, \quad \text{for } k = 3, 6, \lambda \in \text{Gal}\left(\mathbb{Q}(\omega)/\mathbb{Q}\right),
\end{align*}$$

and

$$\begin{align*}
(b/p)(b/\pi)_9 &= (b/\sigma \pi)_{18}, \\
(b/p)(b/\mu)_3 &= (b/\bar{\mu})_6,
\end{align*}$$

$\bar{\mu}$ being the complex conjugate of $\mu$.

Let $g$ be a fixed primitive root mod $p$ and, for $m \not\equiv 0 \pmod{p}$, let $\text{ind} m$ denote the index of $m$ mod $p$ to the base $g$. Define the character $\chi$ on $\mathbb{Z}_p$ (integers modulo $p$) by

$$\chi(m) = \begin{cases} 
\zeta^{\text{ind} m} & \text{if } m \not\equiv 0 \pmod{p}, \\
0 & \text{if } m \equiv 0 \pmod{p}.
\end{cases}$$

Note that for $m \not\equiv 0 \pmod{p}$, $m$ is a ninth power mod $p$ if and only if $\chi(m) = 1$.

For $i, j \mod 9$, define the Jacobi sums of order 9 by

$$J(i, j) = \sum_{v=0}^{p-1} \chi^i(v)\chi^j(v+1) = \sum_{v \not\equiv 0, -1} \zeta^{\text{ind} v + j \text{ind} (v+1)}.$$ 

For $(m, 9) = 1$, we have $J(im, jm) = J(i, j)_{\zeta \to \zeta^m}$. In particular, $J(2, 2) = \sigma J(1, 1)$,
\[ J(4, 4) = \sigma^2 J(1, 1), \quad J(9 - i, 9 - j) = J(-i, -j) = J(i, j). \] For \( i, j, i + j \equiv 0 \pmod{9} \), \( J(i, j) \) are nothing but the sums \( R(i, j, \zeta)_9 \). (See [3, p. 396], [1, p. 207]). Hence from [1, Eq. (3.5)] it follows that
\[ pJ(3, 3) = J(1, 1)\sigma^2 J(1, 1)\sigma^4 J(1, 1). \]

A relation between \( \psi_9(a) \) and \( J(i, j) \) is obtained as follows:
\[
\psi_9(a) = \sum_{x=0}^{p-1} \left( \frac{x^9 + a}{p} \right)
= \sum_{y=0}^{p-1} \left[ 1 + \chi(y) + \chi^2(y) + \ldots + \chi^8(y) \right] \left( \frac{y + a}{p} \right).
\]
Note that \( \sum_{y=0}^{p-1} (y + a)/p = 0 \). In the remaining, set \( y = az \). Therefore,
\[
\psi_9(a) = \left( \frac{a}{p} \right) \left[ \sum_{z=0}^{p-1} \chi(a)\chi(z) \left( \frac{z+1}{p} \right) + \ldots + \sum_{z=0}^{p-1} \chi^8(a)\chi^8(z) \left( \frac{z+1}{p} \right) \right].
\]

Now,
\[
\sum_{z=0}^{p-1} \chi(z) \left( \frac{z+1}{p} \right) = \sum_{z+1 \in R} \chi(z) - \sum_{z+1 \in N} \chi(z).
\]
(Here \( R \) denotes the set of quadratic residues and \( N \) denotes the set of quadratic nonresidues mod \( p \).

But,
\[
0 = \sum_{z+1 \in R} \chi(z) + \sum_{z+1 \in N} \chi(z) + \chi(-1).
\]
Adding,
\[
\sum_{z=0}^{p-1} \chi(z) \left( \frac{z+1}{p} \right) = 2 \sum_{z+1 \in R} \chi(z) + \chi(-1) = \sum_{u=0}^{p-1} \chi(u^2 - 1)
= \sum_{v=0}^{p-1} \chi(4)\chi(v)\chi(v + 1), \quad \text{setting } u = 2v + 1
= \chi(4)J(1, 1).
\]

Similarly,
\[
\sum_{z=0}^{p-1} \chi^i(z) \left( \frac{z+1}{p} \right) = \chi^i(4)J(i, i) \quad \text{for } i = 2, 3, \ldots, 8.
\]

This gives,
\[
(2.3) \quad \psi_9(a) = \left( \frac{a}{p} \right) \sum_{i=1}^{8} \chi^i(4a)J(i, i).
\]
3. Cyclotomy and the congruence for $J(1, 1)$.

For a prime $p \equiv 1 \pmod{3}$ and $i, j \pmod{3}$, Gauss defined the cyclotomic numbers $(i, j)_3$, of order 3, by

$$(i, j)_3 = \text{the number of } v \pmod{p}$$

such that $\text{ind } v \equiv i \pmod{3}$ and $\text{ind } (v + 1) \equiv j \pmod{3}$.

For $p \equiv 1 \pmod{3}$, there are only two integral solutions $(L, \pm M)$ of the equations

$$4p = L^2 + 27M^2, \quad L \equiv 1 \pmod{3},$$

and Gauss showed that $L = 9(1, 2)_3 - p - 1$, whereas $M$ can be taken to be $M = (0, 1)_3 - (0, 2)_3$. For this $M$, he also proved that $18 (0, 1)_3 = 2p - 4 - L + 9M$. (See [3, p. 397]).

Let now, as before, $p \equiv 1 \pmod{9}$. For $i, j \pmod{9}$, the cyclotomic numbers $(i, j)_9$ are defined by

$$(i, j)_9 = \text{the number of } v \pmod{p}$$

such that $\text{ind } v \equiv i \pmod{9}$ and $\text{ind } (v + 1) \equiv j \pmod{9}$.

Following Dickson [5, p. 189], let

$$J(1, 1) = \sum_{i=0}^{5} c_i s_i^i, \quad c_i \in \mathbb{Z}.$$ 

Dickson [5, Eq. 25] showed that

$$c_0 \equiv -1, \quad c_1 \equiv c_2 \equiv -c_4 \equiv -c_5, \quad c_3 \equiv 0 \pmod{3}.$$ (3.1)

K. S. Williams [10, Lemma 1] proved that

$$c_1 \equiv 0 \pmod{3} \quad \text{if } M \equiv 0 \pmod{3}.$$ 

Slightly more generally we have the following

**Lemma 1.** $c_1 \equiv \text{ind } 3 \pmod{3}$.

**Proof.** By Dickson's work [5, p. 189], we have mod 3,

$$c_1 = (0, 1)_9 + (0, 4)_9 - 2(0, 7)_9 + 2(1, 3)_9 - 4(1, 6)_9 + 2(2, 5)_9$$

$$\equiv (0, 1)_9 + (0, 4)_9 + (0, 7)_9 + 2(1, 3)_9 + 2(1, 6)_9 + 2(2, 5)_9$$

$$= (0, 1)_9 + (0, 4)_9 + (0, 7)_9 + (3, 1)_9 + (3, 4)_9 + (3, 7)_9 +$$

$$+ (6, 1)_9 + (6, 4)_9 + (6, 7)_9$$

$$= (0, 1)_3.$$
since
\[(i,j)_3 = \sum_{r,s=0}^{2} (i + 3r, j + 3s),\]

by [5, Eq. 2].

But as \(p \equiv 1 \pmod{9}\), \(L \equiv 7 \pmod{9}\), and in this case, Baumert and Fredricksen proved that \(M \equiv - \text{ind } 3 \pmod{3}\). (See 1, Eq. (3.6)].) Let \(p = 1 + 9n, L = 7 + 9m\), so that,
\[
18c_1 \equiv 18 (0,1)_3 \pmod{27} \\
= 2p - 4 - L + 9M \\
\equiv 2 + 18n - 4 - 7 - 9m - 9 \text{ ind } 3 \pmod{27} \\
\equiv -9 - 9n - 9m - 9 \text{ ind } 3 \pmod{27},
\]

implying that
\[
c_1 \equiv 1 + n + m + \text{ind } 3 \pmod{3}.
\]

Now from Table 2, p. 206 [1], we get,
\[
81(3,6) = \begin{cases} 
  p + 1 + L & \text{if } \text{ind } 3 \equiv 0 \pmod{3}, \\
  p + 1 + L + 27c_0 & \text{if } \text{ind } 3 \equiv 1 \pmod{3}, \\
  p + 1 + L + 27c_0 - 27c_3 & \text{if } \text{ind } 3 \equiv -1 \pmod{3}.
\end{cases}
\]

In any case, \(p + 1 + L \equiv 0 \pmod{27}\). Since \(p + 1 + L = 9(1 + n + m)\), this gives
\[
c_1 \equiv \text{ind } 3 \pmod{3}, \text{ proving the lemma}.
\]

A useful congruence for \(J(1,1)\) is obtained in the following

**Lemma 2.** \(J(1,1) \equiv -\omega^{-\text{ind } 3} \pmod{(1 - \zeta)^4}\).

**Proof.** By (3.1),
\[
J(1,1) \equiv -1 + c_1\zeta + c_1\zeta^2 - c_1\zeta^4 - c_4\zeta^5 \pmod{3} \\
\equiv -1 + c_1\zeta + c_1\zeta^2 - c_1(\zeta^3 + \zeta - 1) - \\
- c_1(\zeta^3 + \zeta^2 - 1) \pmod{(1 - \zeta)^4} \\
\equiv -1 - c_1(1 - \omega) \pmod{3}.
\]

Thus by Lemma 1,
\[
J(1,1) \equiv -1 - (\text{ind } 3)(1 - \omega) \pmod{(1 - \zeta)^4} \\
\equiv -\omega^{-\text{ind } 3} \pmod{3}.
\]
This proves the lemma.

**Remark.** For \( k > 2, i, j \mod k \), and a prime \( p \equiv 1 \mod k \), if we define
\[
J(i, j)_k = \sum_{v=0}^{p-1} r_i \text{ind}_k v + j \text{ind}_k (v+1),
\]
then
\[
J(1, 1)_3 \equiv -1 \mod (1 - \omega)^2 \quad \text{(See e.g. [8, p. 64])},
\]
and
\[
J(1, 1)_k \equiv -1 \mod (1 - \zeta_k)^3 \quad \text{for primes } k > 3 \text{ (See footnote, [4, p. 365])}.
\]

Our Lemma 2 gives the analogue of this to the composite case \( k = 9 \).

4. Statement and proof of the main result.

**Theorem.** Let \( p \) be a rational prime \( \equiv 1 \mod 9 \), \( a \) be an integer \( \equiv 0 \mod p \), \( a\tilde{a} \equiv 1 \mod p \), and \( g \) be a fixed primitive root \( \mod p \). Let \( \pi_0 \) be a prime factor of \( p \) in \( \mathbb{Z}[\zeta] \) satisfying \( g/\pi_0)_9 = \zeta \), and let for the automorphism \( \sigma : \zeta \to \zeta^2 \) of \( \mathbb{Q}(\zeta)/\mathbb{Q} \), \( \pi_i = \sigma^i(\pi_0), \ 0 \leq i \leq 5 \). Assume that \( \pi_0 \) is further normalized by the condition
\[
(4.1) \quad \pi_0 \pi_1 \pi_2 \equiv -1, -\omega, -\omega^2 \mod (1 - \zeta^4),
\]
according as \( \text{ind } 3 \equiv 0, -1, 1 \mod 3 \). Let \( \mu \) denote the prime factor \( \pi_0 \pi_1 \pi_2 \) of \( p \) in \( \mathbb{Q}(\omega) \). Then
\[
(4.2) \quad \varphi_9(a) = -1 + \left( \frac{4\tilde{a}}{\pi_0} \right)_9 \pi_0 \pi_1 \pi_2 + \left( \frac{4\tilde{a}}{\pi_1} \right)_9 \pi_0 \pi_1 \pi_2 + \left( \frac{4\tilde{a}}{\pi_2} \right)_9 \pi_0 \pi_1 \pi_2 + \left( \frac{4\tilde{a}}{\mu} \right)_3 \mu + \left( \frac{4\tilde{a}}{\bar{\mu}} \right)_3 \bar{\mu}
\]

and
ON THE JACOBSHAL SUM $\varphi_9(a)$ AND THE RELATED SUM $\psi_9(a)$

(4.3) \[
\psi_9(a) = \left(\frac{4a}{\pi_1}\right)_{18} \pi_0 \pi_1 \pi_2 + \left(\frac{4a}{\pi_1}\right)_{18} \pi_0 \pi_1 \pi_2 + \]
\[
+ \left(\frac{4a}{\pi_2}\right)_{18} \pi_0 \pi_1 \pi_2 + \left(\frac{4a}{\pi_2}\right)_{18} \pi_0 \pi_1 \pi_2 + \]
\[
+ \left(\frac{4a}{\pi_0}\right)_{18} \pi_0 \pi_1 \pi_2 + \left(\frac{4a}{\pi_0}\right)_{18} \pi_0 \pi_1 \pi_2 + \]
\[
+ \left(\frac{4a}{\bar{\mu}}\right)_{6} \mu + \left(\frac{4a}{\mu}\right)_{6} \bar{\mu}.
\]

(Note that in (4.2), $-1 + (4a/\mu)_3 \mu + (4a/\bar{\mu})_3 \bar{\mu} = \varphi_3(a)$, and similarly in (4.3), $(4a/\bar{\mu})_6 \mu + (4a/\mu)_6 \bar{\mu} = \psi_3(a)$.)

PROOF. (I) We first show that the above normalization of $\pi_0$ is possible, where $\pi_0$ satisfies $(g/\pi_0)_9 = \zeta$.

We have,

\[
J(1,1) = \sum_{v=0}^{p-1} \chi(v) \chi(v+1)
\]
\[
= \sum_{v} \left(\frac{v}{\pi_0}\right)_{9} \left(\frac{v+1}{\pi_0}\right)_{9}, \quad \text{since } (g/\pi_0)_9 = \zeta
\]
\[
\equiv \sum_{v} v^{(p-1)/9} (v+1)^{(p-1)/9} \pmod{\pi_0}
\]
\[
\equiv \sum_{v} v^{(p-1)/9} \left(1 + \frac{p-1}{9} v + \ldots + v^{(p-1)/9}\right)
\]
\[
\equiv 0 \pmod{p}, \quad \text{since } \sum_{v} v^{i} \equiv 0 \pmod{p} \text{ unless } (p-1) | i, i \geq 1.
\]

Thus $\pi_0 | J(1,1)$. Similarly, $\pi_4, \pi_5 | J(1,1)$. Hence $\pi_0 \pi_4 \pi_5 | J(1,1)$, that is $\pi_0 \pi_1 \pi_2 | J(1,1)$. (Note that $\pi_0 = \pi_3$, $\pi_1 = \pi_4$, $\pi_2 = \pi_5$.)

Let $J(1,1) = \pi_0 \pi_1 \pi_2 u$, where $u \in \mathbb{Z}[\zeta]$. So,

\[
\overline{J(1,1)J(1,1)} = \pi_0 \pi_1 \pi_2 \overline{\pi_0 \pi_1 \pi_2 u \bar{u}},
\]
\[
= pu \bar{u},
\]

giving $u \bar{u} = 1$, as $|J(1,1)| = \sqrt{p}$ by [3, Eq. 28]. Hence $u$ is a root of unity.

By Lemma 2, $J(1,1) \equiv -\omega^{-\text{ind}^3} (\mod (1-\zeta)^4)$, showing that there exists $\alpha$ among $\pm 1, \pm \zeta, \ldots, \pm \zeta^8$ such that $\pi_0 \pi_1 \pi_2 \equiv \alpha (\mod (1-\zeta)^4)$. This $\alpha$ is unique because $\pm 1, \pm \zeta, \ldots, \pm \zeta^8$ are incongruent modulo $(1-\zeta)^4$. Thus from the
chosen value of $\pi_0$ find such an $\alpha$. Then $u$ is fixed uniquely by $u = (-\omega^{-\text{ind }3})\alpha^{-1}$.

Now

\[ J(1,1) = \pi_0\sigma^4(\pi_0)\sigma^5(\pi_0)u \]
\[ = \pi_0\sigma^4(\pi_0)\sigma^5(\pi_0)u^7\sigma^4(u^7) \sigma^5(u^7) \]
\[ = (\pi_0u^7)\sigma^4(\pi_0u^7)\sigma^5(\pi_0u^7). \]

Calling $\pi_0u^7$ as new $\pi_0$ we get

\[ J(1,1) = \pi_0\bar{\pi}_1\bar{\pi}_2. \]

Thus we have obtained a prime factor $\pi_0$ of $p$ in $\mathbb{Z}[^{\zeta}]$ such that $(g/\pi_0) = \zeta$ and $\pi_0\bar{\pi}_1\bar{\pi}_2 \equiv -\omega^{-\text{ind }3} \pmod{(1 - \zeta)^4}$. This shows that the required normalization of $\pi_0$ is possible.

(II) Assume that $\pi_0$ is normalized by (4.1). Then in the above, $\alpha = -\omega^{-\text{ind }3}$, $u=1$ and so

\[ J(1,1) = \pi_0\bar{\pi}_1\bar{\pi}_2. \]

From § 2,

\[ J(2,2) = \sigma J(1,1) = \sigma(\pi_0\pi_4\pi_5) = \pi_1\pi_5\pi_0 = \pi_0\pi_1\bar{\pi}_2, \]
\[ J(4,4) = \sigma^2 J(1,1) = \pi_0\pi_1\pi_2. \]

Also, $pJ(3,3) = J(1,1) \cdot \sigma^2 J(1,1) \cdot \sigma^4 J(1,1)$, giving

\[ \pi_0\pi_1\pi_2\pi_3\pi_4\pi_5 J(3,3) = (\pi_0\pi_4\pi_5)(\pi_2\pi_0\pi_1)(\pi_4\pi_2\pi_3). \]

Thus $J(3,3) = \pi_0\pi_2\pi_4$. Denote

\[ \mu = J(3,3) = \pi_0\pi_2\pi_4 = \pi_0\bar{\pi}_1\bar{\pi}_2. \]

$\mu$ is invariant under $\sigma^2$, so $\mu \in \mathbb{Z}[\omega]$.

$\mu\bar{\mu} = p$ shows that $\mu$ is a prime factor of $p$ in $\mathbb{Z}[\omega]$. Hence by (2.3),

\[ (4.4) \quad \psi_9(a) = (a/p)[\chi(4a)\pi_0\bar{\pi}_1\bar{\pi}_2 + \bar{\chi}(4a)\bar{\pi}_0\pi_1\pi_2 + \]
\[ + \chi^2(4a)\pi_0\pi_1\bar{\pi}_2 + \bar{\chi}^2(4a)\bar{\pi}_0\bar{\pi}_1\pi_2 + \]
\[ + \chi^4(4a)\pi_0\pi_1\pi_2 + \bar{\chi}^4(4a)\bar{\pi}_0\pi_1\pi_2 + \]
\[ + \chi^3(4a)\mu + \bar{\chi}^3(4a)\bar{\mu}] . \]

But since $(g/\pi_0)_9 = \zeta$, it follows that

\[ \chi(4a) = (4a/\pi_0)_9 , \]
and by (2.1),
\[ \bar{\chi}(4a) = (4a/\pi_0)_0 \]
\[ \chi^2(4a) = (4a/\pi_1)_0, \quad \bar{\chi}^2(4a) = (4a/\pi_1)_0 \]
\[ \chi^4(4a) = (4a/\pi_2)_0, \quad \bar{\chi}^4(4a) = (4a/\pi_2)_0. \]

Finally it is straightforward to check that
\[ \chi^3(4a) = (4a/\mu)_3, \quad \bar{\chi}^3(4a) = (4a/\bar{\mu})_3. \]

Then, (1.2) and (4.4) prove (4.2), and (2.2) and (4.4) prove (4.3).

This proves the theorem.

**Remark 1.** In the statement of the theorem, instead of defining \( \mu = \pi_0 \pi_1 \pi_2 \),
we could have alternatively defined \( \mu \) to be the prime factor of \( p \) in \( \mathbb{Z} [\omega] \)
determined uniquely by the conditions \( g/\mu_3 = \omega, \mu \equiv -1 \pmod{3} \). This follows
from the work of Rajwade [8], because
\[ J(3,3) = \sum_{v=0,-1} \omega^{\text{ind} v + \text{ind} (v+1)} = J(1,1)_3 \]
\[ = \emptyset \text{ defined in [8].} \]

**Remark 2.** The number of solutions of the congruence \( y^2 \equiv x^9 + a \pmod{p} \),
can be obtained from the relation
\[ N_9(a) = p + \psi_9(a). \]

**Remark 3.** If \( p \) is a prime \( \equiv 4,7 \pmod{9} \), then \( \psi_9(a) = \psi_3(a) \), and this is found
in [7] or [6]. If \( p \equiv 2,5,8 \pmod{9} \) \( (p \neq 2) \), then \( \psi_9(a) = \psi_1(a) = 0 \). Thus one gets
\( \psi_9(a), \varphi_9(a) \) and \( N_9(a) \) in these cases also.

**Remark 4.** One can check that on multiplication by exactly one of
\( \pm \zeta^i (1+\zeta)^j \), \( 0 \leq i \leq 8, 0 \leq j \leq 2 \), \( \pi_0 \) itself can be made to satisfy the condition
\[ \text{(4.5)} \quad \pi_0 \equiv -\omega^{-\text{ind} 3} (\mod{1-\zeta^4}). \]
This condition implies the normalization (4.1) of the theorem, and hence the
conclusions (4.2) and (4.3). However the normalization (4.1) is simpler in the
sense that one needs multiply \( \pi_0 \) just by one of \( \pm \zeta^i \), \( 0 \leq i \leq 8 \), to obtain it.

**Remark 5.** In the proof of our Lemma 1, to prove that \( 1+n+m \equiv 0 \pmod{3} \),
the use of the formulae for \( 81(3,6) \) can be avoided. One can get this result
directly from \( 4p = L^2 + 27M^2 \), \( p = 1+9n \), \( L = 7+9m \). Similar remark holds for
the proof of Lemma 1 of K. S. Williams in [10].
REFERENCES


6. S. A. Katre and A. R. Rajwade, *On the Jacobsthal sum $\varphi_k(a)$ and the related sum $\psi_k(a)$*, to appear.


CENTRE FOR ADVANCED STUDY IN MATHEMATICS
PANJAB UNIVERSITY
CHANDIGARH 160014
INDIA