MATH. SCAND. 53 (1983), 193–202

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

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 $(./p)$ is the Legendre symbol and $a \in \mathbf{Z}$, the ring of rational integers. The sums are easily obtained if $a \equiv 0 \pmod p$, and if $p \not\equiv 1 \pmod k$, they reduce to sums of lower order. These sums are related by

$$\varphi_k(a) = \psi_{2k}(a) - \psi_k(a)\,, \tag{1.1}$$

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

$$\varphi_k(a) = -1 + (a/p)\psi_k(\bar{a})\,, \tag{1.2}$$

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 $\mathbf{Q}(\zeta_k)$ if k is odd and $\mathbf{Q}(\zeta_{2k})$ if k is even, where $\mathbf{Q}$ 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.

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 ζ and ω satisfy the irreducible equations (over $\mathbf{Q}$) $\zeta^6 + \zeta^3 + 1 = 0$ and $\omega^2 + \omega + 1 = 0$, $\mathbf{Z}[\zeta]$ and $\mathbf{Z}[\omega]$ are PID's, $1 - \zeta$ is a prime in $\mathbf{Z}[\zeta]$, and as ideals, $(3) = (1-\zeta)^6$ and $(1-\omega) = (1-\zeta)^3$. Let σ be the automorphism of $\mathbf{Q}(\zeta)$ over $\mathbf{Q}$ such that $\sigma(\zeta) = \zeta^2$. Then

$$\mathrm{Gal}(\mathbf{Q}(\zeta)/\mathbf{Q}) = \{1, \sigma, \sigma^2, \sigma^3, \sigma^4, \sigma^5\} .$$

Let π_0 be any prime factor of p in $\mathbf{Z}[\zeta]$. Then $p = \pi_0\pi_1\pi_2\pi_3\pi_4\pi_5$, where $\pi_i = \sigma^i(\pi_0)$, $0 \leqq i \leqq 5$. For any prime factor π of p in $\mathbf{Z}[\zeta]$ and for $\alpha \in \mathbf{Z}[\zeta]$, we define the ninth power residue symbol $(\alpha/\pi)_9$ by $(\alpha/\pi)_9 = 0, \zeta^i$ if $\alpha^{(p-1)/9} \equiv 0, \zeta^i \pmod \pi$, $0 \leqq i \leqq 8$, and the eighteenth power residue symbol $(\alpha/\pi)_{18}$ by $(\alpha/\pi)_{18} = 0, \pm\zeta^i$ if $\alpha^{(p-1)/18} \equiv 0, \pm\zeta^i \pmod \pi$, $0 \leqq i \leqq 8$. Similarly for a prime factor μ of p in $\mathbf{Z}[\omega]$ and for $\alpha \in \mathbf{Z}[\omega]$ we define $(\alpha/\mu)_3 = 0, 1, \omega, \omega^2$ according as $\alpha^{(p-1)/3} \equiv 0, 1, \omega, \omega^2 \pmod \mu$ and $(\alpha/\mu)_6 = 0, \pm 1, \pm\omega, \pm\omega^2$ according as $\alpha^{(p-1)/6} \equiv 0, \pm 1, \pm\omega, \pm\omega^2 \pmod \mu$. For $b \in \mathbf{Z}$, one can easily prove that

$$(2.1)\qquad \begin{aligned} (b/\lambda\pi)_k &= \lambda(b/\pi)_k, \quad \text{for } k = 9, 18,\ \lambda \in \mathrm{Gal}(\mathbf{Q}(\zeta)/\mathbf{Q}) , \\ (b/\lambda\mu)_k &= \lambda(b/\mu)_k, \quad \text{for } k = 3, 6,\ \lambda \in \mathrm{Gal}(\mathbf{Q}(\omega)/\mathbf{Q}) , \end{aligned}$$

and

$$(2.2)\qquad \begin{aligned} (b/p)(b/\pi)_9 &= (b/\sigma\pi)_{18} , \\ (b/p)(b/\mu)_3 &= (b/\bar{\mu})_6 , \end{aligned}$$

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

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

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

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

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

For $(m, 9) = 1$, we have $J(im, jm) = J(i,j)_{\zeta \to \zeta^m}$. In particular, $J(2,2) = \sigma J(1,1)$,

$J(4,4)=\sigma^2 J(1,1)$, $J(9-i,9-j)=J(-i,-j)=\overline{J(i,j)}$. For $i,j,i+j\not\equiv 0 \pmod 9$, $J(i,j)$ 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:

$$\begin{aligned}\psi_9(a) &= \sum_{x=0}^{p-1}\left(\frac{x^9+a}{p}\right)\\ &= \sum_{y=0}^{p-1}[1+\chi(y)+\chi^2(y)+\ldots+\chi^8(y)]\left(\frac{y+a}{p}\right).\end{aligned}$$

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,

$$\begin{aligned}\sum_{z=0}^{p-1}\chi(z)\left(\frac{z+1}{p}\right) &= 2\sum_{z+1\in R}\chi(z)+\chi(-1) = \sum_{u=0}^{p-1}\chi(u^2-1)\\ &= \sum_{v=0}^{p-1}\chi(4)\chi(v)\chi(v+1), \qquad \text{setting } u=2v+1\\ &= \chi(4)J(1,1) .\end{aligned}$$

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,

$$\psi_9(a) = (a/p)\sum_{i=1}^{8}\chi^i(4a)J(i,i) . \tag{2.3}$$

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

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

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

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 $i, j \bmod 9$, the cyclotomic numbers $(i,j)_9$ are defined by

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

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

Following Dickson [5, p. 189], let

$$J(1,1) = \sum_{i=0}^{5} c_i \zeta^i, \qquad c_i \in Z.$$

Dickson [5, Eq. 25] showed that

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

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

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

Slightly more generally we have the following

LEMMA 1. $c_1 \equiv \operatorname{ind} 3 \pmod 3$.

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

$$\begin{aligned} c_1 &= (0,1)_9 + (0,4)_9 - 2(0,7)_9 + 2(1,3)_9 - 4(1,6)_9 + 2(2,5)_9 \\ &\equiv (0,1)_9 + (0,4)_9 + (0,7)_9 + 2(1,3)_9 + 2(1,6)_9 + 2(2,5)_9 \\ &= (0,1)_9 + (0,4)_9 + (0,7)_9 + (3,1)_9 + (3,4)_9 + (3,7)_9 + \\ &\qquad + (6,1)_9 + (6,4)_9 + (6,7)_9 \\ &= (0,1)_3, \end{aligned}$$

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 $M \equiv -\operatorname{ind} 3 \pmod 3$. (See 1, Eq. (3.6)].) Let $p = 1+9n$, $L = 7+9m$, so that,

$$\begin{aligned} 18c_1 &\equiv 18\ (0,1)_3 \pmod{27} \\ &= 2p-4-L+9M \\ &\equiv 2+18n-4-7-9m-9\operatorname{ind} 3 \pmod{27} \\ &\equiv -9-9n-9m-9\operatorname{ind} 3 \pmod{27} , \end{aligned}$$

implying that

$$c_1 \equiv 1+n+m+\operatorname{ind} 3 \pmod 3 .$$

Now from Table 2, p. 206 [1], we get,

$$81(3,6) = \begin{cases} p+1+L & \text{if } \operatorname{ind} 3 \equiv 0 \pmod 3 , \\ p+1+L+27c_0 & \text{if } \operatorname{ind} 3 \equiv 1 \pmod 3 , \\ p+1+L+27c_0-27c_3 & \text{if } \operatorname{ind} 3 \equiv -1 \pmod 3 . \end{cases}$$

In any case, $p+1+L \equiv 0 \pmod{27}$. Since $p+1+L = 9(1+n+m)$, this gives

$$c_1 \equiv \operatorname{ind} 3 \pmod 3, \text{ proving the lemma .}$$

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

LEMMA 2. $J(1,1) \equiv -\omega^{-\operatorname{ind} 3} \pmod{(1-\zeta)^4}$.

PROOF. By (3.1),

$$\begin{aligned} J(1,1) &\equiv -1+c_1\zeta+c_1\zeta^2-c_1\zeta^4-c_1\zeta^5 \pmod 3 \\ &\equiv -1+c_1\zeta+c_1\zeta^2-c_1(\zeta^3+\zeta-1)- \\ &\qquad -c_1(\zeta^3+\zeta^2-1) \pmod{(1-\zeta)^4} \\ &\equiv -1-c_1(1-\omega) \pmod 3 . \end{aligned}$$

Thus by Lemma 1,

$$\begin{aligned} J(1,1) &\equiv -1-(\operatorname{ind} 3)(1-\omega) \pmod{(1-\zeta)^4} \\ &\equiv -\omega^{-\operatorname{ind} 3} \pmod 3 . \end{aligned}$$

This proves the lemma.

REMARK. For $k>2, i,j \bmod k$, and a prime $p\equiv 1 \bmod k$, if we define

$$J(i,j)_k = \sum_{v=0}^{p-1} \zeta_k^{i \operatorname{ind} v + j \operatorname{ind}(v+1)},$$

then

$$J(1,1)_3 \equiv -1 \bmod (1-\omega)^2 \qquad \text{(See e.g. [8, p. 64])},$$

and

$$J(1,1)_k \equiv -1 \bmod (1-\zeta_k)^3 \qquad \text{for primes } k>3 \text{ (See footnote, [4, p. 365])}.$$

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 $\equiv 1 \pmod 9$, a be an integer $\not\equiv 0 \pmod p$, $a\bar{a}\equiv 1 \pmod p$, and g be a fixed primitive root $\bmod p$. Let π_0 be a prime factor of p in $\mathbf{Z}[\zeta]$ satisfying $(g/\pi_0)_9=\zeta$, and let for the automorphism $\sigma\colon \zeta \to \zeta^2$ of $\mathbf{Q}(\zeta)/\mathbf{Q}$, $\pi_i=\sigma^i(\pi_0)$, $0\leqq i\leqq 5$. Assume that π_0 is further normalized by the condition*

$$\pi_0\bar{\pi}_1\bar{\pi}_2 \equiv -1, -\omega, -\omega^2 \pmod{(1-\zeta)^4}, \tag{4.1}$$

according as $\operatorname{ind} 3 \equiv 0, -1, 1 \pmod 3$. Let μ denote the prime factor $\pi_0\bar{\pi}_1\pi_2$ of p in $\mathbf{Q}(\omega)$. Then

$$\begin{aligned}\varphi_9(a) = -1 &+ \left(\frac{4\bar{a}}{\pi_0}\right)_9 \pi_0\bar{\pi}_1\bar{\pi}_2 + \left(\frac{4\bar{a}}{\bar{\pi}_0}\right)_9 \bar{\pi}_0\pi_1\pi_2 + \\ &+ \left(\frac{4\bar{a}}{\pi_1}\right)_9 \pi_0\pi_1\bar{\pi}_2 + \left(\frac{4\bar{a}}{\bar{\pi}_1}\right)_9 \bar{\pi}_0\bar{\pi}_1\pi_2 + \\ &+ \left(\frac{4\bar{a}}{\pi_2}\right)_9 \pi_0\pi_1\pi_2 + \left(\frac{4\bar{a}}{\bar{\pi}_2}\right)_9 \bar{\pi}_0\bar{\pi}_1\bar{\pi}_2 + \\ &+ \left(\frac{4\bar{a}}{\mu}\right)_3 \mu + \left(\frac{4\bar{a}}{\bar{\mu}}\right)_3 \bar{\mu}\end{aligned} \tag{4.2}$$

and

(4.3)
$$\psi_9(a) = \left(\frac{4a}{\pi_1}\right)_{18}\pi_0\bar{\pi}_1\bar{\pi}_2+\left(\frac{4a}{\bar{\pi}_1}\right)_{18}\bar{\pi}_0\pi_1\pi_2+$$
$$+\left(\frac{4a}{\pi_2}\right)_{18}\pi_0\pi_1\bar{\pi}_2+\left(\frac{4a}{\bar{\pi}_2}\right)_{18}\bar{\pi}_0\bar{\pi}_1\pi_2+$$
$$+\left(\frac{4a}{\bar{\pi}_0}\right)_{18}\pi_0\pi_1\pi_2+\left(\frac{4a}{\pi_0}\right)_{18}\bar{\pi}_0\bar{\pi}_1\bar{\pi}_2+$$
$$+\left(\frac{4a}{\bar{\mu}}\right)_6\mu+\left(\frac{4a}{\mu}\right)_6\bar{\mu}.$$

(Note that in (4.2), $-1+(4\bar{a}/\mu)_3\mu+(4\bar{a}/\bar{\mu})_3\bar{\mu}=\varphi_3(a)$, 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 π_0 is possible, where π_0 satisfies $(g/\pi_0)_9=\zeta$.

We have,

$$\begin{aligned} J(1,1) &= \sum_{v=0}^{p-1}\chi(v)\chi(v+1)\\ &= \sum_v \left(\frac{v}{\pi_0}\right)_9\left(\frac{v+1}{\pi_0}\right)_9, \qquad \text{since } (g/\pi_0)_9 = \zeta\\ &\equiv \sum_v v^{(p-1)/9}(v+1)^{(p-1)/9} \pmod{\pi_0}\\ &= \sum_v v^{(p-1)/9}\left(1+\frac{p-1}{9}v+\ldots+v^{(p-1)/9}\right)\\ &\equiv 0 \pmod p, \qquad \text{since } \sum_v v^i\equiv 0 \pmod p \text{ unless } (p-1)\mid i, i\geqq 1\,. \end{aligned}$$

Thus $\pi_0\mid J(1,1)$. Similarly, $\pi_4,\pi_5\mid J(1,1)$. Hence $\pi_0\pi_4\pi_5\mid J(1,1)$, that is $\pi_0\bar{\pi}_1\bar{\pi}_2\mid J(1,1)$. (Note that $\bar{\pi}_0=\pi_3$, $\pi_1=\pi_4$, $\bar{\pi}_2=\pi_5$.)

Let $J(1,1)=\pi_0\bar{\pi}_1\bar{\pi}_2u$, where $u\in Z[\zeta]$. So,

$$\begin{aligned} J(1,1)\overline{J(1,1)} &= \pi_0\pi_1\pi_2\bar{\pi}_0\bar{\pi}_1\bar{\pi}_2u\bar{u}\,,\\ &= pu\bar{u}\,, \end{aligned}$$

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, $J(1,1)\equiv-\omega^{-\text{ind}\,3} \pmod{(1-\zeta)^4}$, showing that there exists α among $\pm1,\pm\zeta,\ldots,\pm\zeta^8$ such that $\pi_0\bar{\pi}_1\bar{\pi}_2\equiv\alpha \pmod{(1-\zeta)^4}$. This α is unique because $\pm1,\pm\zeta,\ldots,\pm\zeta^8$ are incongruent modulo $(1-\zeta)^4$. Thus from the chosen value of π_0 find such an α. Then u is fixed uniquely by $u=(-\omega^{-\text{ind}\,3})\alpha^{-1}$.

Now

$$\begin{aligned} J(1,1) &= \pi_0\sigma^4(\pi_0)\sigma^5(\pi_0)u \\ &= \pi_0\sigma^4(\pi_0)\sigma^5(\pi_0)u^7\sigma^4(u^7)\sigma^5(u^7) \\ &= (\pi_0 u^7)\sigma^4(\pi_0 u^7)\sigma^5(\pi_0 u^7)\,. \end{aligned}$$

Calling $\pi_0 u^7$ as new π_0 we get

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

Thus we have obtained a prime factor π_0 of p in $\mathbf{Z}[\zeta]$ such that $(g/\pi_0)=\zeta$ and $\pi_0\bar{\pi}_1\bar{\pi}_2 \equiv -\omega^{-\text{ind}\,3}$ (mod $(1-\zeta)^4$). This shows that the required normalization of π_0 is possible.

(II) Assume that π_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,

$$\begin{aligned} J(2,2) &= \sigma J(1,1) = \sigma(\pi_0\pi_4\pi_5) = \pi_1\pi_5\pi_0 = \pi_0\pi_1\bar{\pi}_2\,, \\ J(4,4) &= \sigma^2 J(1,1) = \pi_0\pi_1\pi_2\,. \end{aligned}$$

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

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

μ is invariant under σ^2, so $\mu \in \mathbf{Z}[\omega]$.

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

$$\begin{aligned} \text{(4.4)} \qquad \psi_9(a) = (a/p)[&\chi(4a)\pi_0\bar{\pi}_1\bar{\pi}_2+\bar{\chi}(4a)\bar{\pi}_0\pi_1\pi_2+ \\ &+\chi^2(4a)\pi_0\pi_1\bar{\pi}_2+\bar{\chi}^2(4a)\bar{\pi}_0\bar{\pi}_1\pi_2+ \\ &+\chi^4(4a)\pi_0\pi_1\pi_2+\bar{\chi}^4(4a)\bar{\pi}_0\bar{\pi}_1\bar{\pi}_2+ \\ &+\chi^3(4a)\mu+\bar{\chi}^3(4a)\bar{\mu}]\,. \end{aligned}$$

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

$$\chi(4a) = (4a/\pi_0)_9\,,$$

and by (2.1),

$$\bar{\chi}(4a) = (4a/\bar{\pi}_0)_9$$

$$\chi^2(4a) = (4a/\pi_1)_9, \quad \bar{\chi}^2(4a) = (4a/\bar{\pi}_1)_9$$

$$\chi^4(4a) = (4a/\pi_2)_9, \quad \bar{\chi}^4(4a) = (4a/\bar{\pi}_2)_9 .$$

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 $\mu=\pi_0\bar{\pi}_1\pi_2$, we could have alternatively defined μ to be the prime factor of p in $\mathbf{Z}[\omega]$ determined uniquely by the conditions $(g/\mu)_3=\omega$, $\mu\equiv -1 \pmod 3$. This follows from the work of Rajwade [8], because

$$J(3,3) = \sum_{v=0,\,-1} \omega^{\operatorname{ind} v+\operatorname{ind}(v+1)} = J(1,1)_3$$
$$= \mathfrak{S} \quad \text{defined in [8]} .$$

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 $\pm\zeta^i(1+\zeta)^j$, $0\leqq i\leqq 8$, $0\leqq j\leqq 2$, π_0 itself can be made to satisfy the condition

$$\pi_0 \equiv -\omega^{-\operatorname{ind} 3} \pmod{(1-\zeta)^4} . \tag{4.5}$$

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 π_0 just by one of $\pm\zeta^i$, $0\leqq i\leqq 8$, 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

1. L. D. Baumert and H. Fredricksen, *The cyclotomic numbers of order eighteen with applications to difference sets*, Math. Comp. 21 (1967), 204–219.
2. H. Davenport and H. Hasse, *Die Nullstellen der Kongruenzzetafunktionen in gewissen zyklischen Fallen*, J. Reine Angew. Math. 172 (1935), 151–182.
3. L. E. Dickson, *Cyclotomy, higher congruences and Waring's problem*, Amer. J. Math. 57 (1935), 391–424.
4. L. E. Dickson, *Cyclotomy and trigonomial congruences*, Trans. Amer. Math. Soc. 37 (1935), 363–380.
5. L. E. Dickson, *Cyclotomy when e is composite*, Trans. Amer. Math. Soc. 38 (1935), 187–200.
6. S. A. Katre and A. R. Rajwade, *On the Jacobsthal sum* $\varphi_4(a)$ *and the related sum* $\psi_8(a)$, to appear.
7. P. A. Leonard and K. S. Williams, *Evaluation of certain Jacobsthal sums*, Boll. Un. Mat. Ital. B(5) 15 (1978), 717–723.
8. A. R. Rajwade, *On rational primes p congruent to* 1 (mod 3 *or* 5), Proc. Camb. Philos. Soc. 66 (1969), 61–70.
9. A. R. Rajwade, *On the congruence* $y^2 \equiv x^5 - a \pmod p$, Proc. Camb. Philos. Soc. 74 (1973), 473–475.
10. K. S. Williams, 3 *as a ninth power* (mod p), Math. Scand. 35 (1974), 309–317.

CENTRE FOR ADVANCED STUDY IN MATHEMATICS
PANJAB UNIVERSITY
CHANDIGARH 160014
INDIA