ACTA ARITHMETICA
147.1 (2011)

Jacobi sums and cyclotomic numbers of order l^2

by

Devendra Shirolkar and S. A. Katre (Pune)

1. Introduction. For a positive integer $e \geq 2$, the Jacobi sums of order e are algebraic integers in the cyclotomic field $\mathbb{Q}(\zeta_e)$, where $\zeta_e = \exp(2\pi i/e)$. They are defined in terms of a finite field $\mathbb{F}_q$ with $q = p^r$ where $q \equiv 1 \pmod{e}$, p prime. (See Section 2.) Jacobi sums are important objects in the theory of cyclotomy and their congruences have been studied by many authors. Earlier authors (e.g. [4]) obtained congruences for Jacobi sums defined in terms of $\mathbb{F}_p$, $p \equiv 1 \pmod{e}$, and later authors (e.g. [7]) considered $q \equiv 1 \pmod{e}$.

(1) It is well known (see [4], [12]) that for Jacobi sums of odd prime order l,
$$J(1,j)_l \equiv -1 \pmod{(1-\zeta_l)^2}.$$
This congruence also holds modulo $(1-\zeta_l)^3$. (See [9], [13].)

(2) Congruences for Jacobi sums of order $2l$ (l odd prime) were obtained by V. V. Acharya and S. A. Katre [1]. They showed that
$$J(1,n)_{2l} \equiv -\zeta^{m(n+1)} \pmod{(1-\zeta_l)^2},$$
where n is an odd integer such that $1 \leq n \leq 2l-3$ and $m = \operatorname{ind} 2$.

(3) A congruence for the Jacobi sum $J(1,1)_9$ of order 9 was obtained by S. A. Katre and A. R. Rajwade [10]. They showed that
$$J(1,1)_9 \equiv -1 - (\operatorname{ind} 3)(1-\omega) \pmod{(1-\zeta_9)^4},$$
where $\omega = \zeta_9^3$.

(4) If k is an odd prime power > 3, then (see [8])
$$J(i,j)_k \equiv -1 \pmod{(1-\zeta_k)^3}.$$
R. J. Evans [7] generalised this result to all $k > 2$ by elementary methods, getting sharper congruences in some cases, especially when $k > 8$ is a power of 2.

2010 *Mathematics Subject Classification*: Primary 11T22; Secondary 11T24.
Key words and phrases: Jacobi sums, cyclotomic numbers, congruences, Dickson–Hurwitz sums.

DOI: 10.4064/aa147-1-2

It may be noted that an element α coprime to l in the cyclotomic ring $\mathbb{Z}[\zeta_l]$, l prime, can be uniquely determined if we know its prime ideal decomposition, absolute value and congruence modulo $(1-\zeta_l)^2$. To determine an element in the ring $\mathbb{Z}[\zeta_{l^2}]$ which is coprime to l, the congruence is required modulo $(1-\zeta_{l^2})^{l+1}$. In this sense, the congruences in (1), (2) and (3) above are appropriate congruences which determine the Jacobi sums.

In this paper (see Section 5) for $q = p^r \equiv 1 \pmod{l^2}$, $l > 3$ and p primes, we obtain congruences for Jacobi sums of order l^2 modulo $(1-\zeta)^{l+1}$ in terms of cyclotomic numbers of order l. These are the determining congruences for Jacobi sums of order l^2 and they sharpen the congruences in (4). In Section 6, we obtain cyclotomic numbers of order l^2 in terms of coefficients of Jacobi sums of order l and l^2.

2. Preliminaries. Let e be a positive integer ≥ 2 and $q = p^r \equiv 1 \pmod{e}$, p prime. Let $\mathbb{F}_q$ be a finite field with q elements. Write $p^r = q = ef + 1$. Let ζ be a complex primitive eth root of unity. If γ is a generator of $\mathbb{F}_q^*$ then define the multiplicative character $\chi : \mathbb{F}_q \to \mathbb{Q}(\zeta)$ by $\chi(\gamma) = \zeta$, $\chi(0) = 0$. Given a generator γ of $\mathbb{F}_q^*$ define the *Jacobi sum* by

$$J(i,j) = J(i,j)_e = \sum_{v \in \mathbb{F}_q} \chi^i(v)\chi^j(1+v), \qquad 0 \leq i,j \leq e-1.$$

Here $\chi^0(0) = 0$. Also, i and j can be considered modulo e, with the understanding that $\chi^i(0) = 0$ for any integer i. Note that $J(i,j)_e \in \mathbb{Z}[\zeta]$, the ring of integers of $\mathbb{Q}(\zeta)$.

A variation of the Jacobi sum is defined as

$$J(\chi^i, \chi^j)_e = \sum_{v \in \mathbb{F}_q} \chi^i(v)\chi^j(1-v), \qquad 0 \leq i,j \leq e-1.$$

Observe that $J(i,j)_e = \chi^i(-1)J(\chi^i,\chi^j)_e$. When $q = 2^r$, $\chi^i(-1) = \chi^i(1) = 1$ and both the Jacobi sums coincide. Otherwise $\chi^i(-1) = (-1)^{if}$ and hence the two Jacobi sums differ at most in sign. For multiplicative characters χ and ψ on $\mathbb{F}_q$, $J(\chi,\psi)$ can be analogously defined. The prime ideal decomposition of Jacobi sums is well-known. See [3, p. 346, Corollary 11.2.4] for details.

In the following theorem we state some standard results about Jacobi sums.

THEOREM 2.1 (Elementary properties of Jacobi sums).

(1) *If i and j are congruent to* 0 *modulo e then* $J(\chi^i,\chi^j)_e = q-2$.
(2) *If exactly one of i and j is congruent to* 0 *modulo e then* $J(\chi^i,\chi^j)_e = -1$.

(3) *If i is nonzero modulo e and $i+j$ is congruent to 0 modulo e then* $J(\chi^i,\chi^j)_e = -\chi^i(-1)$.
(4) $J(\chi^i,\chi^j)_e = J(\chi^j,\chi^i)_e = \chi^i(-1)J(\chi^{-i-j},\chi^i)_e$.
(5) *If e divides neither i, j nor $i+j$ then* $|J(\chi^i,\chi^j)_e| = \sqrt{q}$.

Proof. See [4] for $q=p$ and [14] for $q=p^r$. ∎

Remark. If f is even or $q = 2^r$ then $J(i,j)_e = J(\chi^i,\chi^j)_e$, so (4) gives $J(i,j)_e = J(j,i)_e = J(-i-j,j)_e = J(j,-i-j)_e = J(-i-j,i)_e = J(i,-i-j)_e$. In particular $J(i,i)_e = J(-2i,i)_e = J(i,-2i)_e$.

3. Cyclotomy. Let γ, ζ and χ be as in Section 2. For $0\le i,j\le e-1$ ($i,j \pmod e$), define the e^2 cyclotomic numbers $(i,j)_e$ by $(i,j)_e = \mathrm{Card}(X_{ij})$ where

$$\begin{aligned}X_{ij} &= \{v\in\mathbb{F}_q \mid \chi(v)=\zeta^i,\ \chi(v+1)=\zeta^j\}\\ &= \{v\in\mathbb{F}_q-\{0,-1\} \mid \operatorname{ind}_\gamma v\equiv i \pmod e,\ \operatorname{ind}_\gamma(v+1)\equiv j \pmod e\}.\end{aligned}$$

We state some basic properties of the cyclotomic numbers. (See [5] for $q=p$, and [14]). For $q=p^r$,

$$\begin{aligned}(i,j)_e &= (i',j')_e \quad \text{if } i\equiv i' \text{ and } j\equiv j' \pmod e.\\ (i,j)_e &= (e-i,j-i)_e\\ &= \begin{cases}(j,i)_e & \text{if } f \text{ is even or } q=2^r,\\ (j+e/2,i+e/2)_e & \text{otherwise.}\end{cases}\end{aligned}$$

Thus if f is even or $q=2^r$ with $r\ge 2$ then

$$\begin{aligned}(i,j)_e &= (j,i)_e = (i-j,-j)_e = (j-i,-i)_e\\ &= (-i,j-i)_e = (-j,i-j)_e.\end{aligned} \tag{3.1}$$

For e odd >3, the equation (3.1) partitions the e^2 cyclotomic numbers into classes (groups). $(0,0)_e$ forms a singleton class. For $1\le i\le e-1$, $(i,i)_e$, $(0,-i)_e$, and $(-i,0)_e$ form classes of three elements. The remaining cyclotomic numbers are grouped into classes of six elements. ($e=3$ is exceptional; $(1,2)_3=(2,1)_3$ is a class of only two elements.) We also have the following properties. For $e\ge 2$,

$$\sum_{i=0}^{e-1}(i,j)_e = \begin{cases} f-1 & \text{if } j=0,\\ f & \text{if } 1\le j\le e-1.\end{cases} \tag{3.2}$$

If $q=p^r$, p odd prime,

$$\sum_{j=0}^{e-1}(i,j)_e = \begin{cases} f-1 & \text{if } f \text{ is even and } i=0,\\ f-1 & \text{if } f \text{ is odd and } i=e/2,\\ f & \text{otherwise.}\end{cases} \tag{3.3}$$

Also, if $q = 2^r$ then e is odd. In this case

$$\sum_{j=0}^{e-1}(i,j)_e = \begin{cases} f-1 & \text{if } i=0, \\ f & \text{otherwise.} \end{cases} \tag{3.4}$$

In any case,

$$\sum_{i=0}^{e-1}\sum_{j=0}^{e-1}(i,j)_e = q-2. \tag{3.5}$$

Let $q = p^r \equiv 1 \pmod{e}$ and d be any divisor of e. Write $E = e/d$. A cyclotomic number of order E can be expressed as the sum of d^2 cyclotomic numbers of order e by

$$(k,h)_E = \sum_{r=0}^{d-1}\sum_{s=0}^{d-1}(k+rE, h+sE)_e. \tag{3.6}$$

See L. E. Dickson ([6, eq. (2)]) for $q = p$. We will use this formula in Section 5.

4. Relation between Jacobi sums and cyclotomic numbers. The e^2 Jacobi sums and the e^2 cyclotomic numbers are related by

$$\sum_i\sum_j \zeta^{-(ai+bj)}J(i,j)_e = e^2(a,b)_e, \tag{4.1}$$

$$\sum_i\sum_j (i,j)_e\zeta^{ai+bj} = J(a,b)_e. \tag{4.2}$$

Jacobi sums and cyclotomic numbers are related to Dickson–Hurwitz sums. The latter are defined for $i, j \pmod{e}$ by (for $q = p$, see [4])

$$B(i,j) = B(i,j)_e = \sum_{h=0}^{e-1}(h, i-jh)_e. \tag{4.3}$$

They satisfy the relation $B(i,j)_e = B(i, e-j-i)_e$. Also,

$$B(i,0)_e = \begin{cases} f-1 & \text{if } i=0, \\ f & \text{if } 1 \le i \le e-1, \end{cases} \tag{4.4}$$

and

$$\sum_{i=0}^{e-1} B(i,j)_e = q-2. \tag{4.5}$$

Dickson–Hurwitz sums and Jacobi sums $J(\chi, \chi^j)_e$ are related by (for $q = p$, see [4])

$$\chi^j(-1)J(\chi,\chi^j)_e = \chi^j(-1)\chi(-1)J(1,j)_e = \sum_{i=0}^{e-1} B(i,j)_e\zeta^i. \tag{4.6}$$

Hence if f is even or $q = 2^r$ then $J(1,j)_e = \sum_{i=0}^{e-1} B(i,j)_e\zeta^i$.

5. Congruences for Jacobi sums $J(1,n)_{l^2}$ of order l^2. Let $l \geq 3$ be a prime and $q = p^r \equiv 1 \pmod{l^2}$, p prime. Let $\mathbb{F}_q$ be a finite field with q elements. Write $q = l^2 f + 1 = lf' + 1$. Hence $f' \equiv 0 \pmod{l}$. Note also that if p is an odd prime then f and f' are even. Let ζ be a complex primitive l^2th root of unity and $\omega = \zeta^l$. Recall that $(l) = (1-\zeta)^{l(l-1)}$, where $(1-\zeta)$ is a prime ideal in the ring $\mathbb{Z}[\zeta]$. The following lemma determines an element in the ring $\mathbb{Z}[\zeta]$ uniquely.

Lemma 5.1. *Let l be an odd rational prime and ζ be a complex primitive l^2th root of unity. If $\alpha, \beta \in \mathbb{Z}[\zeta]$ are coprime to $(1-\zeta)$ and*

(i) $(\alpha) = (\beta)$,
(ii) $|\alpha| = |\beta|$,
(iii) $\alpha \equiv \beta \pmod{(1-\zeta)^{l+1}}$,

then $\alpha = \beta$.

Proof. $(\alpha) = (\beta)$ implies that $\alpha = \beta u$, where u is a unit in $\mathbb{Z}[\zeta]$. Also $|\alpha| = |\beta|$ gives $u\overline{u} = 1$. Let $u = f(\zeta)$, a polynomial in ζ with coefficients from $\mathbb{Z}$. Therefore $f(\zeta)f(\overline{\zeta}) = 1$ and hence $f(\zeta^i)f(\overline{\zeta^i}) = 1$ for every i relatively prime to l^2. From this it follows that u is a root of unity. But the only roots of unity in $\mathbb{Z}[\zeta]$ are $\pm\zeta^i$. So $u = \pm\zeta^i$, $0 \leq i \leq l^2 - 1$. From condition (iii), $\pm\beta\zeta^i \equiv \beta \pmod{(1-\zeta)^{l+1}}$. Hence

$$\pm\zeta^i \equiv 1 \pmod{(1-\zeta)^{l+1}} \quad (\text{as } \gcd(\beta, (1-\zeta)) = 1).$$

The $-$ sign in the above congruence does not hold as $1+\zeta^i \equiv 2 \pmod{(1-\zeta)}$. Hence $\zeta^i \equiv 1 \pmod{(1-\zeta)^{l+1}}$.

Now, by the binomial theorem, $\zeta^l \equiv 1 + (\zeta-1)^l \pmod{(1-\zeta)^{l+1}}$. Hence $\zeta^l \not\equiv 1 \pmod{(1-\zeta)^{l+1}}$. However $\zeta^{l^2} = 1$. Therefore the order of ζ $\pmod{(1-\zeta)^{l+1}}$ is l^2. Hence $i = 0$. Thus the result follows. ∎

From (4.6), the Jacobi sum $J(1,n)_{l^2} = \sum_{i=0}^{l(l-1)-1} b_{i,n}\zeta^i$ ($b_{i,n} \in \mathbb{Z}$ uniquely determined) of order l^2 is given in terms of Dickson–Hurwitz sums by

$$J(1,n)_{l^2} = \sum_{i=0}^{l^2-1} B(i,n)_{l^2}\zeta^i. \tag{5.1}$$

Here

$$b_{i,n} = B(i,n)_{l^2} - B(l(l-1)+j,n)_{l^2}, \tag{5.2}$$

where $0 \leq j \leq l-1$, and $j \equiv i \pmod{l}$.

Lemma 5.2. *Let $1 \leq u \leq l-1$ and $1 \leq n \leq l^2-1$. Write $n = dl + n'$, $0 \leq n' \leq l-1$. Then*

$$\sum_{i=0}^{l-2} b_{li+u,n} \equiv B(u,n')_l \pmod{l}.$$

Further this sum is zero modulo l if $\gcd(l,n) = l$.

Proof. From (5.2),

$$\begin{aligned}\sum_{i=0}^{l-2} b_{li+u,n} &= \sum_{i=0}^{l-2} B(li+u,n)_{l^2} - (l-1)B(l(l-1)+u,n)_{l^2}\\ &\equiv \sum_{i=0}^{l-1} B(li+u,n)_{l^2} \pmod{l}\\ &= \sum_{i=0}^{l-1}\sum_{a=0}^{l^2-1}(a, li+u-an)_{l^2}\\ &= \sum_{i=0}^{l-1}\sum_{s,t=0}^{l-1}(ls+t, li+u-(ls+t)n)_{l^2}\\ &= \sum_{i=0}^{l-1}\sum_{s,t=0}^{l-1}(ls+t, l(i-sn)+u-nt)_{l^2}\\ &= \sum_{t=0}^{l-1}\sum_{s,i=0}^{l-1}(ls+t, l(i-sn'-dt)+u-n't)_{l^2}\\ &= \sum_{t=0}^{l-1}(t, u-n't)_l \quad \text{using (3.6)}\\ &= B(u,n')_l.\end{aligned}$$

If $\gcd(l,n)=l$ then $n'=0$, and by (4.4), $B(u,0)_l = f' \equiv 0 \pmod{l}$. ∎

LEMMA 5.3. *Let $l>3$ be a prime and $1 \le n \le l^2-1$. Write $n = dl+n'$ as before. For $1 \le h \le l-1$, let*

$$\lambda_h = \lambda_h(n) = \left[\frac{n'h}{l}\right] + \left[\frac{-h(n'+1)}{l}\right],$$

and for $1 \le h,k \le l-1$, $h \ne k$, let

$$\begin{aligned}\lambda_{h,k} = \lambda_{h,k}(n) = \left[\frac{h+n'k}{l}\right] + \left[\frac{k+n'h}{l}\right] + \left[\frac{n'k-h(n'+1)}{l}\right]\\ + \left[\frac{n'h-k(n'+1)}{l}\right] + \left[\frac{k-h(n'+1)}{l}\right] + \left[\frac{h-k(n'+1)}{l}\right].\end{aligned}$$

For a given n, $\lambda_{h,k}$ depends only on the class of six elements (cf. (3.1)) *to which $(h,k)_l$ belongs. Define*

$$S(n) := \sum_{t=0}^{l-1}\sum_{j=0}^{l-1} tB(lt+j,n)_{l^2}.$$

Then

$$S(n) \equiv \sum_{h=1}^{l-1} \lambda_h (h,0)_l + \sum_c \lambda_{h,k}(h,k)_l \pmod{l}$$

where $\sum_c$ *is taken over a set of representatives of classes of six elements of cyclotomic numbers of order* l*, obtained in view of* (3.1)*. Furthermore* $S(n) \equiv 0 \pmod{l}$ *if* $\gcd(l,n) = l$.

Proof. Let $(a,b)_{l^2}$ be a cyclotomic number of order l^2. We count the number of times $(a,b)_{l^2}$ appears in the expression for $S(n)$, and consider this count modulo l. If $(a,b)_{l^2}$ appears in $S(n)$ (in some $B(i,n)_{l^2}$) then it is of the form $(h, i-nh)_{l^2}$ for some $0 \le h, i \le l^2 - 1$. Therefore $a \equiv h \pmod{l^2}$ and $b \equiv i - nh \pmod{l^2}$. Hence we see that $b + na \equiv i \pmod{l^2}$.

Thus, $(a,b)_{l^2} = (h, i-nh)_{l^2}$ comes from exactly one $B(i,n)_{l^2}$ and it is counted as many times as $B(i,n)_{l^2}$ is counted in $S(n)$, i.e. $[i/l]$ times. As $[i/l] \equiv [(b+na)/l] \pmod{l}$, $(a,b)_{l^2}$ is counted $[(b+na)/l]$ times (modulo l) in $S(n)$.

Case (i). Consider the cyclotomic number $(lx, ly)_{l^2}$, where $0 \le x, y \le l-1$. Now we count the number of times this cyclotomic number appears in $S(n)$ in all its different forms with respect to (3.1). $(0,0)_{l^2}$ appears 0 times in $S(n)$.

Subcase (1). If $x = y \ne 0$ then $(lx, ly)_{l^2}$ forms a group of three, namely $(lx, lx)_{l^2} = (0, -lx)_{l^2} = (-lx, 0)_{l^2}$. Hence the number of times $(lx, ly)_{l^2}$ will be counted in these three different forms in $S(n)$ is

$$\equiv \left[\frac{lx + nlx}{l}\right] + \left[\frac{-lxn}{l}\right] + \left[\frac{-lx}{l}\right] \pmod{l} \equiv 0 \pmod{l}.$$

Subcase (2). If $x \ne y$, $x, y \ne 0$ then $(lx, ly)_{l^2}$ forms a group of six (cf. (3.1)), viz.

$$\begin{aligned} (lx, ly)_{l^2} &= (l(x-y), -ly)_{l^2} = (l(y-x), -lx)_{l^2} = (ly, lx)_{l^2} \\ &= (-ly, l(x-y))_{l^2} = (-lx, l(y-x))_{l^2}. \end{aligned}$$

So the number of times this cyclotomic number will be counted in all its six forms is

$$\begin{aligned} &\equiv \left[\frac{lx + nly}{l}\right] + \left[\frac{(x-y)l - nly}{l}\right] + \left[\frac{l(y-x) - nlx}{l}\right] + \left[\frac{ly + nlx}{l}\right] \\ &\quad + \left[\frac{-ly + n(lx - ly)}{l}\right] + \left[\frac{-lx + n(ly - lx)}{l}\right] \pmod{l} \equiv 0 \pmod{l}. \end{aligned}$$

This shows that the contribution to $S(n)$ from all the cyclotomic numbers $(lx, ly)_{l^2}$ corresponding to the cyclotomic number $(0,0)_l$ (cf. (3.6)) is 0 $\pmod{l}$.

Case (ii). Consider a cyclotomic number of the type $(lx+h, ly)_{l^2}$ where $1 \le h \le l-1$ and is fixed, and $0 \le x, y \le l-1$, together with two of its other forms, viz. $(l(y-x)-h, -h-lx)_{l^2}$ and $(-ly, l(x-y)+h)_{l^2}$. The number of times $(lx+h, ly)_{l^2}$ appears in $S(n)$ in these three forms is

$$\begin{aligned}
&\equiv \left[\frac{ly+n(lx+h)}{l}\right] + \left[\frac{-h-lx+n(l(y-x)-h)}{l}\right] \\
&\quad + \left[\frac{l(x-y)+h-ynl}{l}\right] \pmod{l} \\
&\equiv \left[\frac{nh}{l}\right] + \left[\frac{-h(n+1)}{l}\right] \pmod{l} \\
&\equiv \lambda_h \pmod{l}, \qquad \text{putting } n = dl+n'.
\end{aligned}$$

Note that if $y \ne 0$, by (3.1) there are six forms of $(lx+h, ly)_{l^2}$, but we are content with only three mentioned above. The other three forms correspond to $(l(x-y)+h, -ly)_{l^2}$. Hence the contribution to $S(n)$ of $(lx+h, ly)_{l^2}$ with two of its other forms as mentioned is $\lambda_h(lx+h, ly)_{l^2} \pmod{l}$. Hence the total contribution of $(lx+h, ly)_{l^2}$, $(lx-h, ly-h)_{l^2}$ and $(lx, ly+h)_{l^2}$ for all $0 \le x, y \le l-1$ is $\equiv \lambda_h(h, 0)_l \pmod{l}$.

Case (iii). Let $1 \le h, k \le l-1$ with $h \ne k$ be fixed. For any $0 \le x, y \le l-1$ a cyclotomic number $(lx+h, ly+k)_{l^2}$ forms a group of six. Six different forms of this cyclotomic number are

$$\begin{aligned}
(lx+h, ly+k)_{l^2} = (l(x-y)+h-k, -ly-k)_{l^2} &= (l(y-x)+k-h, -lx-h)_{l^2} \\
= (ly+k, lx+h)_{l^2} &= (-ly-k, l(x-y)+h-k)_{l^2} \\
&= (-lx-h, l(y-x)+k-h)_{l^2}.
\end{aligned}$$

So the number of times this cyclotomic number is counted in all its six different forms in $S(n)$ is

$$\begin{aligned}
&\equiv \left[\frac{ly+k+n(lx+h)}{l}\right] + \left[\frac{-ly-k+n(l(x-y)+h-k)}{l}\right] \\
&\quad + \left[\frac{-lx-h+n(l(y-x)+k-h)}{l}\right] + \left[\frac{lx+h+n(ly+k)}{l}\right] \\
&\quad + \left[\frac{l(x-y)+h-k-n(ly+k)}{l}\right] + \left[\frac{l(y-x)+k-h-n(lx+h)}{l}\right] \pmod{l} \\
&= \left[\frac{k+nh}{l}\right] + \left[\frac{-k(n+1)+nh}{l}\right] + \left[\frac{-h(n+1)+nk}{l}\right] \\
&\quad + \left[\frac{h+nk}{l}\right] + \left[\frac{h-k(n+1)}{l}\right] + \left[\frac{k-h(n+1)}{l}\right].
\end{aligned}$$

Putting $n = dl + n'$ we see that

$$\lambda_{h,k} = \left[\frac{h+n'k}{l}\right] + \left[\frac{k+n'h}{l}\right] + \left[\frac{n'k-h(n'+1)}{l}\right] + \left[\frac{n'h-k(n'+1)}{l}\right] + \left[\frac{k-h(n'+1)}{l}\right] + \left[\frac{h-k(n'+1)}{l}\right].$$

Hence the total contribution of $(lx+h, ly+k)_{l^2}$ and of its five other forms for $0 \le x, y \le l-1$ is

$$\sum_{x,y=0}^{l-1} \lambda_{h,k}(lx+h, ly+k)_{l^2} = \lambda_{h,k}(h,k)_l.$$

This ends Case (iii).

Hence by Cases (i)–(iii),

$$S(n) \equiv \sum_{h=1}^{l-1} \lambda_h (h,0)_l + \sum_c \lambda_{h,k}(h,k)_l \pmod{l},$$

where $\sum_c$ is taken over a set of representatives of classes of six elements of cyclotomic numbers of order l, obtained from (3.1).

Now let $n' = 0$, i.e. $(l,n) = l$. Then

$$\lambda_h = \left[\frac{n'h}{l}\right] + \left[\frac{-h(n'+1)}{l}\right] = \left[\frac{-h}{l}\right] = -1,$$

whereas

$$\begin{aligned}\lambda_{h,k} &= \left[\frac{h+n'k}{l}\right] + \left[\frac{k+n'h}{l}\right] + \left[\frac{n'k-h(n'+1)}{l}\right] + \left[\frac{n'h-k(n'+1)}{l}\right] \\ &\quad + \left[\frac{k-h(n'+1)}{l}\right] + \left[\frac{h-k(n'+1)}{l}\right] \\ &= \left[\frac{h}{l}\right] + \left[\frac{k}{l}\right] + \left[\frac{-h}{l}\right] + \left[\frac{-k}{l}\right] + \left[\frac{k-h}{l}\right] + \left[\frac{h-k}{l}\right] = -3.\end{aligned}$$

We use (3.2) and (3.5) to obtain

$$\begin{aligned}S(n) &\equiv -\sum_{h=1}^{l-1}(h,0)_l - 3\sum_c (h,k)_l \pmod{l} \\ &= 1 + (0,0)_l - f' - \frac{1}{2}\sum_c 6(h,k)_l \\ &= 1 - f' + (0,0)_l - \frac{1}{2}\Big(q - 2 - (0,0)_l - 3\sum_{k=1}^{l-1}(k,0)_l\Big) \\ &= 1 - f' + (0,0)_l - \frac{1}{2}(q - 2 - 3(f'-1) + 2(0,0)_l) \\ &= \frac{1}{2}f' - \frac{1}{2}(q-1) \equiv 0 \pmod{l}.\end{aligned}$$

This completes the proof of the lemma. ■

Consider the Jacobi sum of order l^2, $J(1,n)_{l^2} = \sum_{i=0}^{l(l-1)-1} b_{i,n}\zeta^i$. Writing it in powers of $\zeta - 1$ we see that

$$J(1,n)_{l^2} = \sum_{i=0}^{l(l-1)-1} c'_{i,n}(\zeta-1)^i \quad \text{where} \quad c'_{i,n} = \sum_{m=i}^{l(l-1)-1} \binom{m}{i} b_{m,n}.$$

But from Y. Ihara [8, p. 81] (see also R. J. Evans [7]), $J(1,n)_{l^2} \equiv -1 \pmod{(1-\zeta)^3}$. Therefore $c'_{0,n} \equiv -1 \pmod{l}$ and $c'_{1,n} \equiv c'_{2,n} \equiv 0 \pmod{l}$. Hence

$$J(1,n)_{l^2} \equiv -1 + \sum_{i=3}^{l} c'_{i,n}(\zeta-1)^i \pmod{(1-\zeta)^{l+1}}.$$

We shall now get congruences for $c'_{i,n}$ for $3 \le i \le l$. Write $m = lt + u$, $0 \le u \le l-1$ and $0 \le t \le l-2$.

Case 1. Let $3 \le i \le l-1$. Then

$$\binom{m}{i} = \frac{m(m-1)\cdots(m-i+1)}{i!} \equiv \frac{u(u-1)\cdots(u-i+1)}{i!} = \binom{u}{i} \pmod{l},$$

where $\binom{u}{i} = 0$ for $0 \le u < i$. Therefore

$$c'_{i,n} \equiv \sum_{u=i}^{l-1} \left[\binom{u}{i}\Big(\sum_{t=0}^{l-2} b_{lt+u,n}\Big)\right] \pmod{l}.$$

We apply Lemma 5.2 to obtain

$$c'_{i,n} \equiv \sum_{u=i}^{l-1} \left[\binom{u}{i}\Big(\sum_{t=0}^{l-2} b_{lt+u,n}\Big)\right] \equiv \sum_{u=i}^{l-1} \binom{u}{i} B(u,n')_l \pmod{l}.$$

Define, for $3 \le i \le l-1$,

$$c_{i,n} := \sum_{u=i}^{l-1} \binom{u}{i} B(u,n')_l. \tag{5.3}$$

Thus $c'_{i,n} \equiv c_{i,n} \pmod{l}$, $3 \le i \le l-1$.

Case 2. Let $i = l$. Then for $m = lt+u$ as above, $\binom{m}{l} \equiv t \pmod{l}$. Using this observation, from (5.2) we obtain

$$\begin{aligned} c'_{l,n} &= \sum_{m=l}^{l(l-1)-1} \binom{m}{l} b_{m,n} \equiv \sum_{t=0}^{l-2}\sum_{j=0}^{l-1} t b_{lt+j,n} \pmod{l} \\ &= \sum_{t=0}^{l-2}\sum_{j=0}^{l-1} t(B(lt+j,n)_{l^2} - B(l(l-1)+j,n)_{l^2}) \\ &= \sum_{t=0}^{l-2}\sum_{j=0}^{l-1} tB(lt+j,n)_{l^2} - \Big(\sum_{t=0}^{l-2} t\Big)\Big(\sum_{j=0}^{l-1} B(l(l-1)+j,n)_{l^2}\Big). \end{aligned}$$

Now, $-\sum_{t=0}^{l-2} t = -(l-1)(l-2)/2 \equiv l-1 \pmod{l}$. Hence

$$c'_{l,n} \equiv \sum_{t=0}^{l-1}\sum_{j=0}^{l-1} tB(lt+j,n)_{l^2} \pmod{l}.$$

Let λ_h, $\lambda_{h,k}$ and c be as in Lemma 5.3. Define, for $i=l$,

$$c_{l,n} := \sum_{h=1}^{l-1} \lambda_h (h,0)_l + \sum_{c} \lambda_{h,k}(h,k)_l. \tag{5.4}$$

Then by Lemma 5.3,

$$c'_{l,n} \equiv \sum_{t=0}^{l-1}\sum_{j=0}^{l-1} tB(lt+j,n)_{l^2} = S(n) \equiv c_{l,n} \pmod{l}.$$

Thus,

$$J(1,n)_{l^2} \equiv -1 + \sum_{i=3}^{l} c_{i,n}(\zeta-1)^i \pmod{(1-\zeta)^{l+1}}.$$

Furthermore, from Lemmas 5.2 and 5.3, if $l \mid n$ then $c_{i,n} \equiv 0 \pmod{l}$ for $3 \le i \le l$, and we get

$$J(1,n)_{l^2} \equiv -1 \pmod{(1-\zeta)^{l+1}}.$$

We conclude the above discussion in the following theorem.

THEOREM 5.4. *Let $l > 3$ be a prime and $p^r = q \equiv 1 \pmod{l^2}$. If $1 \le n \le l^2-1$, then a (determining) congruence for $J(1,n)_{l^2}$ for a finite field $\mathbb{F}_q$ is given by*

$$J(1,n)_{l^2} \equiv \begin{cases} -1 + \sum_{i=3}^{l} c_{i,n}(\zeta-1)^i \pmod{(1-\zeta)^{l+1}} & \text{if } \gcd(l,n)=1, \\ -1 \pmod{(1-\zeta)^{l+1}} & \text{if } \gcd(l,n)=l, \end{cases}$$

where for $3 \le i \le l-1$, $c_{i,n}$ are described by (5.3) and $c_{l,n} = S(n)$ is given by Lemma 5.3.

REMARK 1. Since Dickson–Hurwitz sums are sums of cyclotomic numbers, for $3 \le i \le l$, $c_{i,n}$ are integral linear combinations of cyclotomic numbers of order l.

REMARK 2. For a given l, the $c_{i,n}$ and hence the above congruence for $J(1,n)_{l^2}$ depends only on $n \pmod{l}$, i.e.

$$J(1,k)_{l^2} \equiv J(1,l+k)_{l^2} \pmod{(1-\zeta)^{l+1}}.$$

REMARK 3. For $\gcd(l,n)=l$, the result in the theorem also follows from the work of R. J. Evans ([7, Thm. 1]).

REMARK 4. The absolute value of the Jacobi sum $J(1,n)_{l^2}$ (see Thm. 2.1(5)) and its prime ideal decomposition (see [3, p. 346, Corollary 11.2.4]) are known. In view of Lemma 5.1, the congruence condition for $J(1,n)_{l^2}$ obtained in Thm. 5.4 together with the absolute value and prime ideal decomposition gives an algebraic characterisation of $J(1,n)_{l^2}$ and hence of all Jacobi sums of order l^2.

REMARK 5. Congruences for Jacobi sums of order l^2 (mod $(1-\zeta)^{l+1}$) could be obtained in terms of cyclotomic numbers of order l. In the same fashion it is expected that the determining congruences for Jacobi sums of order l^m, which are required modulo $(1-\zeta)^{l^{m-1}+1}$, can be obtained in terms of cyclotomic numbers of order l^{m-1} (or of order l^k, $1 \le k \le m-1$). Also appropriate congruences for Jacobi sums of order n may be obtained in terms of cyclotomic numbers of orders d properly dividing n. These expectations are consistent with the result of P. van Wamelen (2002) who gave an algebraic characterization of Jacobi sums of order n in terms of their absolute value, prime ideal decomposition and the Jacobi sums of orders d properly dividing n. (See [15].)

6. Cyclotomic numbers of order l^2. Let l be an odd prime. In this section we obtain formulae for the cyclotomic numbers $(h,k)_{l^2}$ of order l^2 in terms of coefficients of the Jacobi sums of order l^2 and l. Such formulae for cyclotomic numbers of order l, and cyclotomic numbers of order $2l$ were obtained by S. A. Katre and A. R. Rajwade [11], and V. V. Acharya and S. A. Katre [1] respectively.

With the set up of Section 5, write Jacobi sums of order l as $J(1,j)_l = \sum_{i=0}^{l-2} a_{i,j}\omega^i$, where $a_{i,j} \in \mathbb{Z}$. Let $G' = \mathrm{Gal}(\mathbb{Q}(\omega)/\mathbb{Q})$ and $G = \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$. We compute $\mathrm{Tr}_{\mathbb{Q}(\omega)/\mathbb{Q}}(J(1,j)_l\omega^{-t})$. Note that $\mathrm{Tr}_{\mathbb{Q}(\omega)/\mathbb{Q}}(\omega) = -1$. Therefore,

$$\begin{aligned}(6.1)\qquad \mathrm{Tr}_{\mathbb{Q}(\omega)/\mathbb{Q}}(J(1,j)_l\omega^{-t}) &= \mathrm{Tr}_{\mathbb{Q}(\omega)/\mathbb{Q}}\Big(\sum_{i=0}^{l-2} a_{i,j}\omega^{i-t}\Big)\\ &= \sum_{i=0}^{l-2} a_{i,j}\,\mathrm{Tr}_{\mathbb{Q}(\omega)/\mathbb{Q}}(\omega^{i-t}) = la_{t,j} - \sum_{i=0}^{l-2} a_{i,j}.\end{aligned}$$

Similarly, we compute $\mathrm{Tr}_{\mathbb{Q}(\zeta)/\mathbb{Q}}(J(1,n)_{l^2}\zeta^{-t})$. In this case, $\mathrm{Tr}_{\mathbb{Q}(\zeta)/\mathbb{Q}}(\zeta) = 0$, where ζ is any primitive l^2th root of unity, while $\mathrm{Tr}_{\mathbb{Q}(\zeta)/\mathbb{Q}}(\omega) = -l$. Let $B(i,n) = B(i,n)_{l^2}$. Therefore, we have

$$\begin{aligned}(6.2)\qquad \mathrm{Tr}_{\mathbb{Q}(\zeta)/\mathbb{Q}}(J(1,n)_{l^2}\zeta^{-t}) &= \mathrm{Tr}_{\mathbb{Q}(\zeta)/\mathbb{Q}}\Big(\sum_{i=0}^{l^2-1} B(i,n)\zeta^{i-t}\Big)\\ &= \sum_{i=0}^{l^2-1} B(i,n)\,\mathrm{Tr}_{\mathbb{Q}(\zeta)/\mathbb{Q}}(\zeta^{i-t}) = l(l-1)B(t,n) - l\sum_{u=1}^{l-1} B(ul+t,n).\end{aligned}$$

Lemma 6.1. *For t and n modulo l^2, define*

$$C(t,n) := l(l-1)B(t,n) - l\sum_{u=1}^{l-1} B(ul+t,n).$$

Let $0 \le t \le l^2-1$. Write $t = jl+s$, where $0 \le j \le l-1$ and $0 \le s \le l-1$. Then

$$C(t,n) = \epsilon(t)b_{t,n} - l\sum_{u=0}^{l-2} b_{ul+t,n}, \quad \textit{where}$$

$$\epsilon(t) = \begin{cases} l^2 & \textit{if } 0 \le j \le l-2, \textit{ i.e. } 0 \le t < l(l-1), \\ -l & \textit{if } j = l-1, \textit{ i.e. } l(l-1) \le t \le l^2-1. \end{cases}$$

Proof. (i) Let $0 \le j \le l-2$. Then

$$\begin{aligned} C(t,n) &= l(l-1)B(t,n) - l\sum_{u=1}^{l-1} B(ul+t,n) \\ &= l(l-1)B(jl+s,n) - l\sum_{u=1}^{l-1} B((u+j)l+s,n) \\ &= l(l-1)B(jl+s,n) - l(l-1)B(l(l-1)+s,n) \\ &\quad + l(l-2)B(l(l-1)+s,n) - l\sum_{u=1}^{l-j-2} B((u+j)l+s,n) \\ &\quad - l\sum_{u=l-j}^{l-1} B((u+j)l+s,n) \\ &= l(l-1)(B(jl+s,n) - B(l(l-1)+s,n)) \\ &\quad - l\sum_{u=1}^{l-2-j} (B((u+j)l+s,n) - B(l(l-1)+s,n)) \\ &\quad - l\sum_{u=l-j}^{l-1} (B((u+j)l+s,n) - B(l(l-1)+s,n)). \end{aligned}$$

In the first sum put $u+j = x$, and in the second put $u+j \equiv x \pmod{(l-1)}$. Hence using (5.2) we get

$$\begin{aligned} C(t,n) = l(l-1)&(B(jl+s,n) - B(l(l-1)+s,n)) \\ &- l\sum_{x=0}^{j-1}(B(xl+s,n) - B(l(l-1)+s,n)) \\ &- l\sum_{x=j+1}^{l-2} (B(xl+s,n) - B(l(l-1)+s,n)) \end{aligned}$$

$$= l(l-1)b_{jl+s,n} - l\sum_{x=j+1}^{l-2} b_{xl+s,n} - l\sum_{x=0}^{j-1} b_{xl+s,n}$$
$$= l^2 b_{jl+s,n} - l\sum_{x=0}^{l-2} b_{xl+s,n} = l^2 b_{t,n} - l\sum_{x=0}^{l-2} b_{xl+s,n}.$$

For every u, we have $ul+t \equiv xl+s \pmod{l(l-1)}$ for some $x \in \{0,\dots,l-2\}$. Therefore

$$C(t,n) = l^2 b_{t,n} - l\sum_{u=0}^{l-2} b_{ul+t,n}.$$

(ii) Let $j = l-1$. Then

$$C(t,n) = l(l-1)B(t,n) - l\sum_{u=1}^{l-1} B(ul+t,n)$$
$$= l(l-1)B(l(l-1)+s,n) - l\sum_{u=1}^{l-1} B((u-1+l)l+s,n)$$
$$= -l\sum_{u=1}^{l-1}(B((u-1+l)l+s,n) - B(l(l-1)+s,n))$$
$$= -l\sum_{u=1}^{l-1}(B((u-1)l+s,n) - B(l(l-1)+s,n))$$
$$= -l\sum_{x=0}^{l-2}(B(xl+s,n) - B(l(l-1)+s,n)).$$

Again, using (5.2),

$$C(t,n) = -l\sum_{x=0}^{l-2} b_{xl+s,n} = -l\sum_{u=0}^{l-2} b_{ul+t,n}.$$

So from (i) and (ii) above we get

$$C(t,n) = \epsilon(t)b_{t,n} - l\sum_{u=0}^{l-2} b_{ul+t,n}, \quad \text{where} \tag{6.3}$$

$$\epsilon(t) = \begin{cases} l^2 & \text{if } 0 \le j \le l-2, \text{ i.e. } 0 \le t < l(l-1), \\ -l & \text{if } j = l-1, \text{ i.e. } l(l-1) \le t \le l^2-1. \end{cases} \blacksquare$$

Now we observe that

$$\sum_{i=1}^{(l^2-1)/2} (\zeta^{-it} + \zeta^{it}) = \begin{cases} l^2-1 & \text{if } t = 0, \\ -1 & \text{otherwise.} \end{cases}$$

Therefore,

$$\begin{aligned}
&\sum_{i=1}^{(l^2-1)/2} J(i,0)(\zeta^{ih}+\zeta^{-ih}+\zeta^{-ik}+\zeta^{ik}+\zeta^{-ih+ik}+\zeta^{ih-ik})\\
&\quad=-\sum_{i=1}^{(l^2-1)/2}(\zeta^{ih}+\zeta^{-ih})-\sum_{i=1}^{(l^2-1)/2}(\zeta^{ik}+\zeta^{-ik})-\sum_{i=1}^{(l^2-1)/2}(\zeta^{ih-ik}+\zeta^{-ih+ik})\\
&\quad=3+\delta(h,k),
\end{aligned}$$

where $\delta(h,k)$ is given by

$$\delta(h,k)=\begin{cases}-3l^2 & \text{if } h\equiv k\equiv 0 \pmod{l^2},\\ -l^2 & \text{if exactly one of } h,k,h-k \text{ is} \equiv 0 \pmod{l^2},\\ 0 & \text{if } h,k,h-k\not\equiv 0 \pmod{l^2}.\end{cases}$$

From (4.1), (6.1), (6.2) and Lemma 6.1 we get the following

THEOREM 6.2. *Let p be a prime and $p^r=q\equiv 1 \pmod{l^2}$. Then the cyclotomic numbers $(h,k)_{l^2}$ of order l^2 are given in terms of coefficients of the Jacobi sums of order l and order l^2 by*

$$\begin{aligned}
l^4(h,k)_{l^2}&=q+1+\delta(h,k)+l\sum_{j=1}^{l-2}a_{h+jk,j}-\sum_{j=1}^{l-2}\sum_{i=0}^{l-2}a_{i,j}-l\sum_{j=1}^{l^2-2}\sum_{u=0}^{l-2}b_{ul+h+jk,j}\\
&\quad-l\sum_{i=1}^{l-2}\sum_{u=0}^{l-2}b_{ul+hil+k,li}+\sum_{j=1}^{l^2-2}\epsilon(h+jk)b_{h+jk,j}+\sum_{i=1}^{l-2}\epsilon(hil+k)b_{hil+k,li}.
\end{aligned}$$

Proof. Write $q=1+l^2f$. Now either f is even and $q=p^r$, p odd; or f is odd and $q=2^r$. Hence by the Remark in Section 2 we get

$$\begin{aligned}
l^4(h,k)_{l^2}&=\sum_{i,j=0}^{l^2-1}J(i,j)_{l^2}\zeta^{-ih-jk}\qquad\text{(from (4.1))}\\
&=J(0,0)_{l^2}+\sum_{i=1}^{(l^2-1)/2}J(i,0)_{l^2}(\zeta^{ih}+\zeta^{-ih}+\zeta^{-ik}+\zeta^{ik}+\zeta^{-ih+ik}+\zeta^{ih-ik})\\
&\quad+\sum_{j=1}^{l-2}\sum_{\sigma\in G'}\sigma(J(1,j)_l\omega^{-h-jk})+\sum_{j=1}^{l^2-2}\sum_{\sigma\in G}\sigma(J(1,j)_{l^2}\zeta^{-h-jk})\\
&\quad+\sum_{i=1}^{l-1}\sum_{\sigma\in G}\sigma(J(il,1)_{l^2}\zeta^{-lih-k})
\end{aligned}$$

$$
\begin{aligned}
&= q + 1 + \delta(h,k) + \sum_{j=1}^{l-2} \mathrm{Tr}_{\mathbb{Q}(\omega)/\mathbb{Q}}(J(1,j)_l \omega^{-h-jk}) \quad \text{(from above)} \\
&\quad + \sum_{j=1}^{l^2-2} \mathrm{Tr}_{\mathbb{Q}(\zeta)/\mathbb{Q}}(J(1,j)_{l^2} \zeta^{-h-jk}) + \sum_{i=1}^{l-1} \mathrm{Tr}_{\mathbb{Q}(\zeta)/\mathbb{Q}}(J(1,li)_{l^2} \zeta^{-lih-k}) \\
&= q + 1 + \delta(h,k) + \sum_{j=1}^{l-2} \Big(l a_{h+jk,j} - \sum_{i=0}^{l-2} a_{i,j} \Big) \quad \text{(from (6.1))} \\
&\quad + \sum_{j=1}^{l^2-2} \mathrm{Tr}_{\mathbb{Q}(\zeta)/\mathbb{Q}} \Big(\sum_{i=0}^{l^2-1} B(i,j) \zeta^{i-h-jk} \Big) + \sum_{i=1}^{l-1} \mathrm{Tr}_{\mathbb{Q}(\zeta)/\mathbb{Q}} \Big(\sum_{j=0}^{l^2-1} B(j,li) \zeta^{j-lih-k} \Big) \\
&= q + 1 + \delta(h,k) + l \sum_{j=1}^{l-2} a_{h+jk,j} - \sum_{i=0}^{l-2} \sum_{j=1}^{l-2} a_{i,j} \\
&\quad + \sum_{j=1}^{l^2-2} \mathrm{Tr}_{\mathbb{Q}(\zeta)/\mathbb{Q}} \Big(\sum_{t=0}^{l^2-1} B(t+h+jk,j) \zeta^{t} \Big) \\
&\quad + \sum_{i=1}^{l-1} \mathrm{Tr}_{\mathbb{Q}(\zeta)/\mathbb{Q}} \Big(\sum_{t=0}^{l^2-1} B(t+lih+k,li) \zeta^{t} \Big) \\
&= q + 1 + \delta(h,k) + l \sum_{j=1}^{l-2} a_{h+jk,j} - \sum_{j=1}^{l-2} \sum_{i=0}^{l-2} a_{i,j} \\
&\quad + \sum_{j=1}^{l^2-2} \Big[l(l-1) B(h+jk,j) - l \sum_{x=1}^{l-1} B(xl+h+jk,j) \Big] \\
&\quad + \sum_{i=1}^{l-1} \Big[l(l-1) B(lih+k,li) - l \sum_{x=1}^{l-1} B(xl+hil+k,li) \Big] \quad \text{(from (6.2))} \\
&= q + 1 + \delta(h,k) + l \sum_{j=1}^{l-2} a_{h+jk,j} - \sum_{j=1}^{l-2} \sum_{i=0}^{l-2} a_{i,j} \\
&\quad + \sum_{j=1}^{l^2-2} C(h+jk,j) + \sum_{i=1}^{l-1} C(hil+k,li) \\
&= q + 1 + \delta(h,k) + l \sum_{j=1}^{l-2} a_{h+jk,j} - \sum_{j=1}^{l-2} \sum_{i=0}^{l-2} a_{i,j} - l \sum_{j=1}^{l^2-2} \sum_{u=0}^{l-2} b_{ul+h+jk,j} \\
&\quad - l \sum_{i=1}^{l-2} \sum_{u=0}^{l-2} b_{ul+hil+k,li} + \sum_{j=1}^{l^2-2} \epsilon(h+jk) b_{h+jk,j} + \sum_{i=1}^{l-2} \epsilon(hil+k) b_{hil+k,li},
\end{aligned}
$$

where the last equality is obtained using Lemma 6.1. ∎

REMARK. For cyclotomic numbers of order 9 see also [2].

Acknowledgements. The first author would like to thank the Council of Scientific and Industrial Research (C.S.I.R.), New Delhi, India for financial support during his research study. The authors thank Bhaskaracharya Pratisthana, an Institute of Mathematics in Pune, India, for providing certain facilities.

References

[1] V. V. Acharya and S. A. Katre, *Cyclotomic numbers of orders $2l$, l an odd prime*, Acta Arith. 69 (1995), 51–74.
[2] L. D. Baumert and H. Fredricksen, *The cyclotomic numbers of order eighteen with applications to difference sets*, Math. Comp. 21 (1967), 204–219.
[3] B. C. Berndt, R. J. Evans, and K. S. Williams, *Gauss and Jacobi Sums*, Wiley, New York, 1998.
[4] L. E. Dickson, *Cyclotomy and trinomial congruences*, Trans. Amer. Math. Soc. 37 (1935), 363–380.
[5] —, *Cyclotomy, higher congruences, and Waring's problem*, Amer. J. Math. 57 (1935), 391–424.
[6] —, *Cyclotomy when e is composite*, Trans. Amer. Math. Soc. 38 (1935), 187–200.
[7] R. J. Evans, *Congruences for Jacobi sums*, J. Number Theory 71 (1998), 109–120.
[8] Y. Ihara, *Profinite braid groups, Galois representations, and complex multiplications*, Ann. of Math. 123 (1986), 43–106.
[9] K. Iwasawa, *A note on Jacobi sums*, in: Symposia Math. 15, Academic Press, London, 1975, 447–459.
[10] S. A. Katre and A. R. Rajwade, *On the Jacobsthal sum $\phi_9(a)$ and the related sum $\psi_9(a)$*, Math. Scand. 53 (1983), 193–202.
[11] —, —, *Complete solution of the cyclotomic problem in $\mathbb{F}_q$ for any prime modulus l, $q = p^\alpha$, $p \equiv 1 \pmod{l}$*, Acta Arith. 45 (1985), 183–199.
[12] J. C. Parnami, M. K. Agrawal, and A. R. Rajwade, *Jacobi sums and cyclotomic numbers for a finite field*, ibid. 41 (1982), 1–13.
[13] —, —, —, *A congruence relation between the coefficients of the Jacobi sum*, Indian J. Pure Appl. Math. 12 (1981), 804–806.
[14] T. Storer, *Cyclotomy and Difference Sets*, Markham, Chicago, 1967.
[15] P. van Wamelen, *Jacobi sums over finite fields*, Acta Arith. 102 (2002), 1–20.

Devendra Shirolkar, S. A. Katre
Department of Mathematics
University of Pune
Pune 411007, India
E-mail: dshirolkar@gmail.com
sakatre@math.unipune.ac.in

Received on 28.5.2009
and in revised form on 21.3.2010 (6043)