ACTA ARITHMETICA
LXIX.1 (1995)

Cyclotomic numbers of order $2l$, l an odd prime

by

Vinaykumar V. Acharya and S. A. Katre (Pune)

1. Introduction. Let e be a positive integer ≥ 2 and p be a rational prime $\equiv 1 \pmod{e}$. Let $q = p^\alpha$ and $\mathbb{F}_q$ be the finite field of q elements. Write $q = ef + 1$. Let γ be a generator of the cyclic group $\mathbb{F}_q^*$. Let ξ be a primitive (complex) eth root of unity. Define a character χ on $\mathbb{F}_q^*$ by $\chi(\gamma) = \xi$ and put $\chi(0) = 0$ for convenience. (Note that for any integer i, positive, negative or zero, $\chi^i(0)$ is to be taken as 0.) For $0 \leq i, j \leq e-1$ (or rather for i, j modulo e) define the e^2 cyclotomic numbers $A_{i,j}$ (also written in the literature as (i,j)) by

$$A_{i,j} = \text{cardinality of } X_{i,j}, \tag{1}$$

where

$$\begin{aligned} X_{i,j} &= \{v \in \mathbb{F}_q \mid \chi(v) = \xi^i, \chi(v+1) = \xi^j\} \\ &= \{v \in \mathbb{F}_q - \{0,-1\} \mid \operatorname{ind}_\gamma v \equiv i \pmod{e}, \operatorname{ind}_\gamma(v+1) \equiv j \pmod{e}\}. \end{aligned} \tag{2}$$

Also define the e^2 Jacobi sums $J(i,j)$ by

$$J(i,j) = \sum_{v \in \mathbb{F}_q} \chi^i(v)\chi^j(v+1). \tag{3}$$

The Jacobi sums $J(i,j)$ and the cyclotomic numbers $A_{i,j}$ are related by

$$\sum_i \sum_j \xi^{-(ai+bj)} J(i,j) = e^2 A_{a,b} \quad \text{and} \quad \sum_i \sum_j A_{i,j}\xi^{ai+bj} = J(a,b). \tag{4}$$

These relations show that if we want to determine all the $A_{i,j}$ it is sufficient to determine all the Jacobi sums $J(i,j)$. Also note that if we change the generator of $\mathbb{F}_q^*$, then the sets $X_{i,j}$ get interchanged among themselves and so also the cyclotomic numbers $A_{i,j}$ and the Jacobi sums $J(i,j)$.

The problem of determining cyclotomic numbers in terms of the solutions of certain diophantine systems (the so-called cyclotomic problem) has been treated by different authors since the time of Gauss (1801). The cyclotomic numbers of prime order l in the finite field $\mathbb{F}_q$, $q = p^\alpha$, $p \equiv 1 \pmod{l}$ have been treated by Gauss ($l = 3, q = p$), Dickson ($l = 5, q = p$), Leonard and

Williams ($l = 7, 11, q = p$), Parnami, Agrawal and Rajwade ($l \leq 19, q = p^\alpha$) and Katre and Rajwade (any $l, q = p^\alpha$). See [6] and the references therein. There was certain ambiguity in the work of Gauss, Dickson etc. which has been removed by Katre and Rajwade in [6] thereby obtaining a complete solution of the cyclotomic problem for any prime modulus l. In fact the removal of the ambiguity has helped in treating the problem in the general l-case.

A number of authors have considered cyclotomic numbers of small composite orders and their work again involves the classical ambiguity, and the problem of removal of the ambiguity may also be taken up for composite moduli. The first general case which may be taken up would be that of modulus $2l$, where l is an odd prime. (For $l = 2$, i.e. $2l = 4$, see [7].) The reason for this preference is that the cyclotomic numbers of order l as well as $2l$ are related to the same cyclotomic field, viz. $\mathbb{Q}(\zeta)$, $\zeta = \exp(2\pi i/l)$, and it is therefore expected that the system of diophantine equations considered in the l-case would also be useful in the $2l$-case. The cyclotomic numbers of order $e = 2l$ have earlier been treated by Dickson ($e = 6$, $q = p$ in detail; $e = 10, 14$, $q = p$ sketchy) [3], [4], A. L. Whiteman ($e = 10, q = p$, treated in sufficient details) [11], Muskat ($e = 14$, $q = p$) [8], N. Buck and K. S. Williams ($e = 14, q = p$) [2] and Zee ($e = 22$, $q = p$, partially) [12], Berndt and Evans [1] ($e = 6, 10$, $q = p^2$), M. Hall ($e = 6$, $q = p^\alpha$) [5], Storer ($e = 6$, $q = p^\alpha$) [10]. The results of these authors involve the classical ambiguity discussed in [6]. Roughly speaking, the considered diophantine system has more solutions than required and a unique solution of the system needs to be chosen which would give the correct formulae for the cyclotomic numbers corresponding to the given generator of $\mathbb{F}_q^*$.

The aim of the present paper is to determine the cyclotomic numbers of order $2l$ in terms of the solutions of the diophantine system considered for the l-case (see equations (i) and (ii) in §6) except that the proper choice of the solutions for the $2l$-case is made by additional conditions (iii), (iv)$'$, (v)$'$, (vi)$'$ which replace the conditions (iii), (iv), (v), (vi) (see §6) used in the l-case. These additional conditions determine required unique solutions thereby also giving arithmetic characterisation of the relevant Jacobi sums and then the cyclotomic numbers of order $2l$ are determined unambiguously by the formulae (23). We have thus also shown how the cyclotomic numbers of order l and $2l$ can be treated simultaneously. (We recall that the cyclotomic numbers of order 10 were obtained by Whiteman in terms of the solutions of the same diophantine system which was used by Dickson to treat the cyclotomic numbers of order 5. Similarly the cyclotomic numbers of order 14 were obtained by Muskat in terms of the same diophantine system which was used earlier by Dickson to treat the cyclotomic numbers of order 7.)

We have to mention that a number of calculations of Whiteman [11] and Muskat [8] were useful in deriving the formulae for cyclotomic numbers of order $2l$ (see §5).

As an illustration, in §7 we give an unambiguous evaluation of cyclotomic numbers of order 6 in $\mathbb{F}_q$ in terms of the solutions of the diophantine system hitherto considered by Gauss, Dickson, M. Hall and Storer.

2. Cyclotomic numbers of order $2l$. Let $e = 2l$, l an odd prime. Let $A_{i,j}$ denote cyclotomic numbers of order $2l$ for any given generator γ of $\mathbb{F}_q^*$. Observe that

$$\sum_{i=0}^{2l-1}\sum_{j=0}^{2l-1} A_{i,j} = q-2.$$

Also,

$$\sum_{j=0}^{2l-1} A_{i,j} = f - n_i, \tag{5}$$

where $n_i = 1$ if $i = 0$, f even or if $i = l$, f odd; and $n_i = 0$ otherwise. Further,

$$\sum_{i=0}^{2l-1} A_{i,j} = \begin{cases} f-1 & \text{if } j = 0, \\ f & \text{otherwise.} \end{cases} \tag{6}$$

Now if f is even then $v \in X_{i,j}$ if and only if $-v-1 \in X_{j,i}$ if and only if $-v/(v+1) \in X_{i-j,2l-j}$ if and only if $-(v+1)/v \in X_{j-i,2l-i}$.

Again if f is odd then $v \in X_{i,j}$ if and only if $-v-1 \in X_{j+l,i+l}$ if and only if $-v/(v+1) \in X_{l+i-j,2l-j}$ if and only if $-(v+1)/v \in X_{j-i+l,l-i}$.

Thus if f is even we have

$$A_{i,j} = A_{j,i} = A_{i-j,-j} = A_{j-i,-i} = A_{-i,j-i} = A_{-j,i-j}, \tag{7}$$

and if f is odd we have

$$A_{i,j} = A_{j+l,i+l} = A_{l+i-j,-j} = A_{l+j-i,l-i} = A_{-i,j-i} = A_{l-j,i-j}. \tag{8}$$

3. Jacobi sums of order $2l$ and their properties. In this section we give some elementary properties of Jacobi sums $J(i,j)$ of order $2l$.

Let ζ and ξ be primitive lth and $2l$th roots of unity in terms of which the character χ and the Jacobi sums $J_l(i,j)$ and $J(i,j) = J_{2l}(i,j)$ of order l and $2l$ (resp.) are defined. Assume moreover that they satisfy $\zeta = \xi^2$ (or equivalently $\xi = -\zeta^{(l+1)/2}$). This assumption is required especially when the Jacobi sums of order l and $2l$ are simultaneously considered. (See e.g. (5) of Proposition 1 below.) This notation will prevail throughout the remaining part of the paper unless stated otherwise.

PROPOSITION 1. (1) *If* $a+b+c \equiv 0 \pmod{2l}$ *then*

$$J(a,b) = J(c,b) = \chi^c(-1)J(c,a) = \chi^a(-1)J(b,c) = \chi^a(-1)J(a,c) = \chi^c(-1)J(b,a).$$

In particular, $J(1,a) = \chi(-1)J(1,2l-a-1)$.

(2) $J(0,j) = \begin{cases} -1 & \text{if } j \not\equiv 0 \pmod{2l}, \\ q-2 & \text{if } j \equiv 0 \pmod{2l} \end{cases}$,

$J(i,0) = -\chi^i(-1)$ *if* $i \not\equiv 0 \pmod{2l}$.

(3) *Let* $a+b \equiv 0 \pmod{2l}$ *but not both zero* $\pmod{2l}$. *Then* $J(a,b) = -1$.

(4) *For* $(k,2l)=1$, $\tau_k J(i,j) = J(ik,jk)$, *where* τ_k *is the automorphism* $\xi \mapsto \xi^k$ *of* $\mathbb{Q}(\zeta)$ *over* $\mathbb{Q}$. *In particular, if for* $(i,2l)=1$, i^{-1} *denotes the inverse of* i *modulo* $2l$ *then* $\tau_{i^{-1}} J(i,j) = J(1,ji^{-1})$.

(5) $J(2r,2s) = J_l(r,s)$ *where* $J_l(r,s)$ *are the Jacobi sums of order* l.

(6) $J(1,n)\overline{J(1,n)} = \begin{cases} q & \text{if } n \not\equiv 0,-1 \pmod{2l}, \\ 1 & \text{if } n \equiv 0,-1 \pmod{2l}. \end{cases}$

(7) (Product Rule for Jacobi sums) *Let* m, n, t *be integers such that* $m+n \not\equiv 0 \pmod{2l}$ *and* $m+t \not\equiv 0 \pmod{2l}$. *Then*

$$J(m,n)J(m+n,t) = \chi^m(-1)J(m,t)J(n,m+t).$$

Proof. The proof of properties (1)–(5) follows using the definition of the Jacobi sum. The proof of (6) is analogous to the proof in the l-case (see [9]). To prove (7), consider

$$\begin{aligned} J(m,n)J(m+n,t) &= \Big\{ \sum_{v\in\mathbb{F}_q} \chi^m(v)\chi^n(v+1) \Big\} \Big\{ \sum_{u\in\mathbb{F}_q} \chi^{m+n}(u)\chi^t(u+1) \Big\} \\ &= \sum_{u\in\mathbb{F}_q^*} \Big\{ \sum_{v\in\mathbb{F}_q} \chi^m(uv)\chi^n(uv+u) \Big\} \chi^t(u+1) \\ &= S_1 + S_2, \end{aligned}$$

say, where S_1 and S_2 are defined below.

For every $u \neq 0$, there is a unique $v \in \mathbb{F}_q$ such that $uv+u+1=0$, i.e. $v = -(u+1)/u$. The total contribution from such pairs (u,v) is S_2, where

$$\begin{aligned} S_2 &= \sum_{u\in\mathbb{F}_q^*, v=-(u+1)/u} \chi^m(uv)\chi^n(uv+u)\chi^t(u+1) \\ &= \sum_{u\in\mathbb{F}_q^*} \chi^m(-u-1)\chi^n(-1)\chi^t(u+1) \\ &= \sum_{u\in\mathbb{F}_q^*} \chi^{m+n}(-1)\chi^{m+t}(u+1) = -\chi^{m+n}(-1)\chi^{m+t}(1) = -\chi^{m+n}(-1), \end{aligned}$$

as $m+t \not\equiv 0 \pmod{2l}$. The remaining part of the above sum is S_1, where

$$S_1 = \sum_{u\in\mathbb{F}_q^*, v\neq -(u+1)/u} \{\chi^m(uv)\chi^n(uv+u)\}\chi^t(u+1).$$

Now there is a bijection between the $(q-1)^2$ pairs (u,v) satisfying $u\neq 0$, $v\neq -(u+1)/u$ and the $(q-1)^2$ pairs (x,y) satisfying $y\neq -1$, $x\neq -y/(y+1)$, the correspondence being given by $x=-uv/(uv+u+1)$ and $y=uv+u$, with the inverse transformations $u=x+y+xy$ and $v=-(x+xy)/(x+y+xy)$. Hence

$$\begin{aligned} S_1 &= \chi^m(-1)\sum_{y\neq -1}\sum_{x\neq -y/(y+1)} \{\chi^m(xy+x)\chi^n(y)\}\chi^t((x+1)(y+1)) \\ &= \chi^m(-1)\sum_{y\neq -1}\sum_{x\neq -y/(y+1)} \chi^m(x)\chi^{m+t}(y+1)\chi^n(y)\chi^t(x+1). \end{aligned}$$

Now

$$\begin{aligned} &\chi^m(-1)\sum_{y\neq -1, x\neq -y/(y+1)} \chi^m(x)\chi^{m+t}(y+1)\chi^n(y)\chi^t(x+1) \\ &\quad = \chi^m(-1)\sum_{y\neq -1}\chi^m(-y/(y+1))\chi^{m+t}(y+1)\chi^n(y)\chi^t(1/(y+1)) \\ &\quad = \sum_{y\neq -1}\chi^{m+n}(y) = -\chi^{m+n}(-1) \quad (\text{as } m+n\not\equiv 0 \pmod{2l}) \\ &\quad = -\chi^{m+n}(-1). \end{aligned}$$

Hence

$$S_1 = \chi^m(-1)\sum_{y\neq -1}\sum_x \chi^m(x)\chi^{m+t}(y+1)\chi^n(y)\chi^t(x+1) + \chi^{m+n}(-1).$$

Thus

$$\begin{aligned} S_1+S_2 &= \chi^m(-1)\sum_{y\neq -1}\sum_x \chi^m(x)\chi^{m+t}(y+1)\chi^n(y)\chi^t(x+1) \\ &= \chi^m(-1)\sum_x\{\chi^m(x)\chi^t(x+1)\}\Big\{\sum_{y\neq -1}\chi^n(y)\chi^{m+t}(y+1)\Big\} \\ &= \chi^m(-1)J(m,t)J(n,m+t). \end{aligned}$$

R e m a r k. It follows that all the $4l^2$ Jacobi sums of order $2l$ are known if the Jacobi sums of order l are known and also the Jacobi sums $J(1,n)$, $1\le n\le 2l-3$, n odd (or equivalently as somebody else may prefer $J(1,n)$, $1\le n\le 2l-2$, n even). Now Jacobi sums of order l are known if $J_l(1,n)$ are known for $1\le n\le (l-3)/2$ ($J(1,1)$ for $l=3$), see [9]. It thus follows that it is sufficient to determine $J(1,n)$ for $1\le n\le 2l-3$, n odd and $J_l(1,n)$ for $1\le n\le (l-3)/2$ ($J_l(1,1)$ for $l=3$).

4. Technical lemmas. This section deals with prime ideal decomposition of the Jacobi sums of order $2l$ (see Lemmas 1, 2 and Proposition 2) and their important congruence property (Proposition 3). These results may also be derived using Gauss sums, and especially the congruence property for $J(1,n)$ (Proposition 3) may be obtained using the relation about Gauss sums considered by Dickson ([3], p. 407 to be considered more generally for $q=p^\alpha$). However we have given the proofs within the framework of Jacobi sums only.

As in the previous section, $J(i,j)$ denotes a Jacobi sum of order $2l$ whereas $J_l(i,j)$ denotes a Jacobi sum of order l; also ζ, ξ are as before with $\zeta=\xi^2$.

Recall that as $p\equiv 1 \pmod l$, p splits completely in $\mathbb{Z}[\zeta]$ and is a product of $l-1$ distinct prime ideals in $\mathbb{Z}[\zeta]$. If $\wp$ is any one of these prime ideals, then $(p)=\prod_{(k,2l)=1}\wp^{\tau_k}=\prod_{(k,l)=1}\wp^{\sigma_k}$, where $\sigma_k\in \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ such that $\sigma_k(\zeta)=\zeta^k$.

Lemma 1. *Let $p\equiv 1 \pmod l$, l an odd prime (thus $p\equiv 1 \pmod{2l}$). Let $b=\gamma^{(q-1)/l}$ and $c=\gamma^{(q-1)/2l}$. Then $b,c\in\mathbb{F}_p$. Let b', c' be integers such that $b'=b$ in $\mathbb{F}_p$ and $c'=c$ in $\mathbb{F}_p$. Let $B=N_{\mathbb{Q}(\zeta)/\mathbb{Q}}(b'-\zeta)$ and $C=N_{\mathbb{Q}(\zeta)/\mathbb{Q}}(c'-\xi)$. Then $B\equiv 0 \pmod p$ and $C\equiv 0 \pmod p$. Further there is a unique prime divisor $\wp$ of p in $\mathbb{Z}[\zeta]$ which divides $b'-\zeta$ and there is a unique prime divisor $\wp'$ of p in $\mathbb{Z}[\zeta]$ which divides $c'-\xi$. Moreover, $\wp=\wp'$.*

Proof. $c^{2l}=\gamma^{q-1}=1$ and the equation $x^{2l}=1$ has exactly $2l$ roots in $\mathbb{F}_p$ as $2l\,|\,(p-1)$, so $c\in\mathbb{F}_p$. Further,

$$B=N_{\mathbb{Q}(\zeta)/\mathbb{Q}}(b'-\zeta)=(b'-\zeta)(b'-\zeta^3)\dots(b'-\zeta^{2l-1})=(b'^l-1)/(b'-1).$$

Hence $B\equiv 0 \pmod p$. Also,

$$C=N_{\mathbb{Q}(\zeta)/\mathbb{Q}}(c'-\xi)=(c'-\xi)(c'-\xi^3)\dots(c'-\xi^{2l-1})=(c'^l+1)/(c'+1).$$

Hence $C\equiv 0 \pmod p$.

It follows at once that there are prime divisors $\wp$, $\wp'$ of p which divide $b'-\zeta$ and $c'-\xi$ respectively. If $\wp$ and $\wp_1$ are different prime divisors of p which divide $b'-\zeta$ then $\wp=\wp_1^\sigma$, where $\sigma\in\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$. Clearly $\sigma\neq 1$ and we have $b'-\zeta\equiv 0 \pmod\wp$ and $b'-\zeta\equiv 0 \pmod{\wp_1}$. This gives $b'-\zeta^\sigma\equiv 0 \pmod{\wp_1^\sigma}$, i.e. $b'-\zeta^\sigma\equiv 0 \pmod\wp$. Hence $\zeta-\zeta^\sigma\equiv 0 \pmod\wp$. Taking norms we get $l\equiv 0 \pmod p$, a contradiction. This proves the uniqueness of $\wp$. Similarly we can prove the uniqueness of $\wp'$. Also $b'\equiv c'^2 \pmod p$ and so $b'-\zeta\equiv c'^2-\xi^2 \pmod{p\mathbb{Z}[\zeta]}$, i.e. $b'-\zeta\equiv(c'-\xi)(c'+\xi) \pmod{p\mathbb{Z}[\zeta]}$. Hence $\wp'$ divides $b'-\zeta$ and so $\wp'=\wp$.

Lemma 2. *Let $\wp$ be as in Lemma 1 and τ_k as in Proposition 1. Let k be an integer such that $1\le k\le 2l-1$, $(k,2l)=1$ and let n be any integer.*

Then $J(1,n)^{\tau_k} \equiv 0 \pmod{\wp}$ *if and only if* $\Lambda((n+1)k) > k$, *where* $\Lambda(r)$ *is defined as the least non-negative residue of* r *modulo* $2l$.

P r o o f. Consider the expression

$$S_k = \sum_{v \in \mathbb{F}_q} v^{k(q-1)/2l}(v+1)^{nk(q-1)/2l}.$$

This is in $\mathbb{F}_p$ as each term is in $\mathbb{F}_p$. Clearly $S_k = S_{k+2l}$. We claim that $S_k = 0$ in $\mathbb{F}_p$ if and only if $\Lambda((n+1)k) > k$. This is done as follows:

$$\begin{aligned} S_k &= \sum_{v \in \mathbb{F}_q} (v-1)^{k(q-1)/2l} v^{nk(q-1)/2l} \\ &= \sum_{v \in \mathbb{F}_q} \sum_{j=0}^{k(q-1)/2l} v^{(k(q-1)/2l)-j}(-1)^j v^{nk(q-1)/2l} \binom{k(q-1)/2l}{j} \\ &= \sum_{v \in \mathbb{F}_q} \sum_{j=0}^{k(q-1)/2l} (-1)^j v^{(k(n+1)(q-1)/2l)-j} \binom{k(q-1)/2l}{j}. \end{aligned}$$

Let $h = \Lambda((n+1)k)$. Hence

$$S_k = \sum_{j=0}^{k(q-1)/2l} (-1)^j \sum_{v \in \mathbb{F}_q} v^{(h(q-1)/2l)-j} \binom{k(q-1)/2l}{j}.$$

Note that

$$\sum_{v \in \mathbb{F}_q} v^j = \begin{cases} 0 & \text{if } (q-1) \nmid j, \\ q-1 & \text{if } (q-1) \mid j. \end{cases}$$

Now for $0 \le j < q-1$, $(q-1) \mid \{(h(q-1)/2l)-j\}$ if and only if $j = h(q-1)/2l$. Hence $S_k = 0$ if $h > k$. Also for $h \le k$,

$$S_k = -(-1)^{h(q-1)/2l} \binom{k(q-1)/2l}{h(q-1)/2l}.$$

Further, as $q = p^\alpha$, the exact power of p dividing $(x(q-1)/2l)!$ is

$$(x(q-1)/2l(p-1)) - (\alpha x/2l).$$

Hence for $h \le k$ the exact power of p dividing

$$\binom{k(q-1)/2l}{h(q-1)/2l}$$

is

$$\begin{aligned} (k(q-1)/2l(p-1)) - (\alpha k/2l) - (h(q-1)/2l(p-1)) + (\alpha h/2l) \\ -((k-h)(q-1)/2l(p-1)) - (\alpha(k-h)/2l) = 0, \end{aligned}$$

so that $S_k \neq 0$. Thus $S_k = 0$ in $\mathbb{F}_p$ if and only if $\Lambda((n+1)k) > k$.

Let c' be an integer as in Lemma 1. Let $T_k = \sum'_{v\in\mathbb{F}_q} c'^{k \operatorname{ind} v + nk \operatorname{ind}(v+1)}$. (Here $\sum'$ signifies that the values $v = 0, -1$ are omitted in the summation.) Then $T_k = S_k$ in $\mathbb{F}_p$. Now consider

$$\begin{aligned} J(1,n)^{\tau_k} - T_k &= \sum_{v\in\mathbb{F}_q} \chi^k(v)\chi^{nk}(v+1) - \sum_{v\in\mathbb{F}_q}{}' c'^{k \operatorname{ind} v + nk \operatorname{ind}(v+1)} \\ &= \sum_{v\in\mathbb{F}_q}{}' \{\chi^k(v)\chi^{nk}(v+1) - \chi^k(v)c'^{nk \operatorname{ind}(v+1)}\} \\ &\quad + \sum_{v\in\mathbb{F}_q}{}' \{\chi^k(v)c'^{nk \operatorname{ind}(v+1)} - c'^{k \operatorname{ind} v + nk \operatorname{ind}(v+1)}\}. \end{aligned}$$

Here each term gives out a factor $c' - \xi$ in $\mathbb{Z}[\zeta]$. But as $T_k = S_k$ in $\mathbb{F}_p$, $T_k \equiv 0 \pmod p$ if and only if $\Lambda((n+1)k) > k$. So $J(1,n)^{\tau_k} \equiv 0 \pmod{\wp}$ if and only if $\Lambda((n+1)k) > k$.

Note 1. Let $U = \{k \mid 1 \le k \le 2l-1, (k, 2l) = 1\}$. Then U has $l-1$ elements. Let $n \equiv 0 \pmod{2l}$. Then for any k in this set, $\Lambda((n+1)k) = k$. Thus for any $k \in U$, $J(1,n)^{\tau_k} \not\equiv 0 \pmod{\wp}$. This is in conformity with the result $J(i,0) = -\chi^i(-1)$ (see (2) of Proposition 1). Further let $n \equiv -1 \pmod{2l}$. Then for any $k \in U$, $\Lambda((n+1)k) = 0 < k$, so that $J(1,n)^{\tau_k} \not\equiv 0 \pmod{\wp}$. This agrees with $J(1, 2l-1) = -1$. (See (3) of Proposition 1.)

Note 2. Let $n \not\equiv 0, -1 \pmod{2l}$. Let $k \in U$. As $n \not\equiv 0 \pmod{2l}$, $\Lambda((n+1)k) \ne k$. As $n \not\equiv -1 \pmod{2l}$, $\Lambda((n+1)k) \ne 0$, so $\Lambda((n+1)k) > k$ if and only if $\Lambda((n+1)(2l-k)) < 2l-k$. Hence for $n \not\equiv 0, -1 \pmod{2l}$, the subsets of U defined by $U_n = \{k \mid \Lambda((n+1)k) > k\}$ and $U'_n = \{k \mid \Lambda((n+1)k) < k\} = \{2l-k \mid \Lambda((n+1)k) > k\}$ each have $(l-1)/2$ elements. U_n and U'_n are disjoint and their union is U.

Proposition 2. *For $n \not\equiv 0, -1 \pmod{2l}$,*

$$(J(1,n)) = \prod_{\Lambda((n+1)k)>k} (\wp^{\tau_{k^{-1}}})^{\alpha}. \tag{9}$$

Proof. As $n \not\equiv 0, -1 \pmod{2l}$, by Proposition 1, $J(1,n)\overline{J(1,n)} = q = p^{\alpha}$. Thus the prime divisors of $J(1,n)$ must come from prime divisors of p. Let U be as in Note 1 above. For $k \in U$, $J(1,n)^{\tau_k} \equiv 0 \pmod{\wp}$ if and only if $J(1,n) \equiv 0 \pmod{\wp^{\tau_{k^{-1}}}}$ and by Lemma 2, this happens if and only if $\Lambda((n+1)k) > k$. Thus by Note 2, there are exactly $(l-1)/2$ prime divisors of p which also divide $J(1,n)$. As $\overline{J(1,n)} = J(1,n)^{\tau_{-1}}$, $\overline{J(1,n)}$ also has exactly $(l-1)/2$ prime divisors, which moreover divide p. As $J(1,n)\overline{J(1,n)} = q = p^{\alpha}$, and as p has $l-1$ distinct prime divisors we see that $(J(1,n))$ and $(\overline{J(1,n)})$ are coprime ideals and so each prime divisor $\wp^{\tau_{k^{-1}}}$ of $J(1,n)$ must divide $J(1,n)$ α times. This gives us (9).

LEMMA 3.

$$J(i,l) = \chi^i(4)J(i,i). \tag{10}$$

P r o o f. If $u \in \mathbb{F}_q$, the number of $v \in \mathbb{F}_q$ satisfying $v(v+1) = u$ is equal to $1+\chi^l(1+4u)$. (Note that χ^l is nothing but the quadratic residue symbol for $\mathbb{F}_q$.) Thus

$$\begin{aligned} J(i,i) &= \sum_{v\in\mathbb{F}_q} \chi^i(v(v+1)) = \sum_{u\in\mathbb{F}_q} \chi^i(u)(1+\chi^l(1+4u)) \\ &= \chi^{-i}(4) \sum_{u\in\mathbb{F}_q} \chi^i(4u)\chi^l(1+4u) = \chi^{-i}(4)J(i,l). \end{aligned}$$

PROPOSITION 3. *Let n be an odd integer such that $1 \le n \le 2l-3$ and let $m = \operatorname{ind}_\gamma 2$. Then*

$$J(1,n) \equiv -\zeta^{-m(n+1)} \pmod{(1-\zeta)^2}. \tag{11}$$

P r o o f. We first prove (11) for $n = l$. By Lemma 3 we have $J(1,1) = \zeta^{-m}J(1,l)$. By (7) of Proposition 1 we get,

$$J(1,n)J(1+n,l-1) = \chi(-1)J(1,l-1)J(n,l).$$

But by (1) of Proposition 1, $\chi(-1)J(1,l-1) = J(1,l)$ so that we have

$$J(1,n)J(1+n,l-1) = J(1,l)J(n,l).$$

In particular, for $n = 1$, we get $J(1,l)J(1,l) = J(1,1)J(2,l-1)$. Note that $J(2,l-1) = J_l(1,(l-1)/2)$. Now recall from Lemma 4, §2 of [9] that for $1 \le n \le l-2$,

$$J_l(1,n) \equiv -1 \pmod{(1-\zeta)^2}. \tag{11}'$$

This gives $J(2,l-1) = J_l(1,(l-1)/2) \equiv -1 \pmod{(1-\zeta)^2}$. Hence using $J(1,1) = \zeta^{-m}J(1,l)$, we get $J(1,l) \equiv -\zeta^{-m} \pmod{(1-\zeta)^2}$. This proves (11) for $n = l$.

Next suppose $n \ne l$. Thus $(n,2l) = 1$. Now as obtained above

$$J(1,n)J(n+1,l-1) = J(1,l)J(n,l) = J(1,l)\tau_n J(1,l).$$

But

$$J(1+n,l-1) = J_l((1+n)/2,(l-1)/2) \equiv -1 \pmod{(1-\zeta)^2},$$

using (11)′. Hence using the congruence for $J(1,l)$ we get (11) in this case also. Thus (11) is valid for all odd n, $1 \le n \le 2l-3$.

R e m a r k. If n is even, $2 \le n \le 2l-2$, using $J(1,n) = \chi(-1)J(1,2l-n-1)$, we get $J(1,n) \equiv -\chi(-1)\zeta^{mn} \pmod{(1-\zeta)^2}$.

LEMMA 4. *Let $\alpha, \beta \in \mathbb{Z}[\zeta]$, both prime to $1-\zeta$, satisfy* (i) $(\alpha) = (\beta)$, (ii) $|\alpha| = |\beta|$, (iii) $\alpha \equiv \beta \pmod{(1-\zeta)^2}$. *Then $\alpha = \beta$.*

P r o o f. See e.g. Lemma 5, §2 of Parnami, Agrawal and Rajwade [9].

Remark. In view of Lemma 4, Proposition 2, Proposition 1(6) and Proposition 3 (resp. Remark after Proposition 3) give an algebraic characterization of $J(1,n)$ for $1 \le n \le 2l-2$, n odd (resp. n even).

5. Dickson–Hurwitz sums, Jacobi sums and the cyclotomic numbers of order $2l$. The evaluation of the cyclotomic numbers of order l in terms of coefficients of certain Jacobi sums has been done in Lemma 5 of Katre and Rajwade [6]. We state it here for convenience.

Proposition 4 (Katre–Rajwade). *Let* $J_l(1,n) = \sum_{i=1}^{l-1} a_i(n)\zeta^i$. *Then the cyclotomic numbers of order* l *are given by*

$$l^2 A_{(i,j)_l} = q - 3l + 1 + \varepsilon(i) + \varepsilon(j) + \varepsilon(i-j) + l\sum_{n=1}^{l-2} a_{in+j}(n) - \sum_{n=1}^{l-2}\sum_{k=1}^{l-1} a_k(n),$$

where

$$a_0(n) = 0, \qquad \varepsilon(i) = \begin{cases} 0 & \text{if } l \mid i, \\ l & \text{otherwise}, \end{cases}$$

and the subscripts in $a_{in+j}(n)$ *are considered modulo* l.

The aim of this section is the evaluation of the cyclotomic numbers of order $2l$ in terms of the coefficients of the Jacobi sums $J_l(1,n) = \sum_{i=1}^{l-1} a_i(n)\zeta^i$, $1 \le n \le l-2$, and $J_{2l}(1,n) = \sum_{i=1}^{l-1} b_i(n)\zeta^i$, $1 \le n \le 2l-1$, n odd. (One may compare if necessary the results of this section with those in [8] and [11] at places.) To do this we first consider Dickson–Hurwitz sums of order $2l$, $B_{2l}(j,n) = B(j,n)$, which are defined for j, n modulo $2l$ by

$$B(j,n) = \sum_{i=0}^{2l-1} A_{(i,j-ni)_{2l}}. \tag{12}$$

They satisfy the following relations:

$$B(j,n) = B(j, 2l-n-1), \tag{13}$$

$$B(j,0) = \begin{cases} f-1 & \text{if } 2l \mid j, \\ f & \text{if } 2l \nmid j, \end{cases}$$

$$\sum_{j \text{ even}} B(j,n) = (q-3)/2,$$

$$\sum_{j \text{ odd}} B(j,n) = (q-1)/2. \tag{14}$$

(Cf. eqs. (2.12), (2.13), (5.10) of Whiteman [11] obtained for $q = p$.) In terms of $B(j,n)$ we can write $J(nm,m)$ as $J(nm,m) = \sum_{j=0}^{2l-1} B(j,n)\xi^{mj}$. (Cf. eq. (2.8) of [11].) Thus $J(n,1) = \sum_{j=0}^{2l-1} B(j,n)\xi^j$. Define the Jacobi differences $D(j,n) = B(j,n) - B(j+l,n)$. Clearly $D(j,n) = D(j,2l-n-1)$. Now

$J(nm,m) = \sum_{j=0}^{l-1} D(2j,n)\zeta^{mj}$ and hence, in particular, we have $J(n,1) = \sum_{j=0}^{l-1} D(2j,n)\zeta^j$. If we assume that n is odd, then by Proposition 1(1), we get $J(1,n) = J(n,1)$. Thus for n odd,

$$J(1,n) = \sum_{j=0}^{l-1} D(2j,n)\zeta^j. \tag{15}$$

The Jacobi differences $D(j,n)$ are obtained in terms of $b_i(n)$ in the following proposition.

PROPOSITION 5. *Let* $J_{2l}(1,n) = \sum_{i=1}^{l-1} b_i(n)\zeta^i$. *Let* n *be an odd integer. Then*

$$\sum_{i=1}^{l-1} b_i(n) = -(1 + lD(0,n)). \tag{16}$$

Moreover,

$$lD(j,n) = (-1)^j \Big(lb_{\nu(j)}(n) - 1 - \sum_{i=1}^{l-1} b_i(n) \Big), \tag{17}$$

where

$$\nu(j) = \begin{cases} \Lambda(j)/2 & \text{if } j \text{ is even}, \\ \Lambda(j+l)/2 & \text{if } j \text{ is odd}, \end{cases}$$

$\Lambda(r)$ *being defined as the least non-negative residue of* r *modulo* $2l$.

P r o o f. As n is odd, by (15) we have $J_{2l}(1,n) = \sum_{i=0}^{l-1} D(2i,n)\zeta^i$. Comparing this with $J_{2l}(1,n) = \sum_{i=1}^{l-1} b_i(n)\zeta^i$, we get $D(2i,n) - D(0,n) = b_i(n)$. Summing over i we get $\sum_{i=1}^{l-1} b_i(n) = -(1+lD(0,n))$, as $\sum_{i=0}^{l-1} D(2i,n) = -1$ by (14). Hence we get

$$lD(2j,n) = \Big(lb_j(n) - 1 - \sum_i b_i(n) \Big).$$

As $D(j,n) = -D(j+l,n)$, we get

$$lD(j,n) = (-1)^j \Big(lb_{\nu(j)}(n) - 1 - \sum_i b_i(n) \Big).$$

In the next proposition we obtain $B_{2l}(j,n)$ for n odd, in terms of $a_i(n)$ and $b_i(n)$, just for record.

PROPOSITION 5′. *For* n *odd*,

$$\begin{aligned} 2lB_{2l}(j,n) &= la_j(n) + q - 2 - \sum_{i=1}^{l-1} a_i(n) + (-1)^j \Big(lb_{\nu(j)}(n) - 1 - \sum_{i=1}^{l-1} b_i(n) \Big). \end{aligned} \tag{17′}$$

Proof. Using (12) and the fact that

$$A_{(i,j)_l} = A_{(i,j)_{2l}} + A_{(i,j+l)_{2l}} + A_{(i+l,j)_{2l}} + A_{(i+l,j+l)_{2l}}$$

we get

$$B_l(j,n) = B_{2l}(j,n) + B_{2l}(j+l,n).$$

Now $D(j,n) = B(j,n) - B(j+l,n)$. Also, from Lemma 5 of [6], we have

$$lB_l(j,n) = la_j(n) + q - 2 - \sum_{i=1}^{l-1} a_i(n).$$

Hence using (17) we get (17)′.

We now determine $A_{(i,j)_{2l}}$ in terms of the a_i's and b_i's. Following Whiteman [11] we define

$$s(i,j) = A_{(i,j)_{2l}} - A_{(i,j+l)_{2l}} \quad \text{and} \quad t(i,j) = A_{(i,j)_{2l}} - A_{(i+l,j)_{2l}}.$$

Lemma 5. *Let l be an odd prime. Then*

$$4A_{(i,j)_{2l}} = A_{(i,j)_l} + s(i,j) + s(i+l,j) + 2t(i,j).$$

Proof. Since $A_{(i,j)_l} = A_{(i,j)_{2l}} + A_{(i,j+l)_{2l}} + A_{(i+l,j)_{2l}} + A_{(i+l,j+l)_{2l}}$ we get the above result.

Remark.

$$t(i,j) = \begin{cases} s(j,i) & \text{if } f \text{ is even,} \\ s(j+l,i+l) & \text{if } f \text{ is odd.} \end{cases} \tag{18}$$

As $A_{(i,j)_l}$ are known in terms of the coefficients of $J_l(1,n)$ (see Proposition 4), to obtain $A_{(i,j)_{2l}}$ we shall first, in Proposition 6, obtain $s(i,j)$ in terms of the Jacobi differences $D(j,n)$. As $D(j,n) = D(j,2l-n-1)$ and as $D(j,n), n$ odd, are known in terms of the coefficients of $J_{2l}(1,n)$, n odd (see (17)), we get $A_{(i,j)_{2l}}$ in terms of the coefficients of $J_l(1,n)$ and in terms of the coefficients of $J_{2l}(1,n)$, n odd. This has been achieved in Proposition 7.

Proposition 6. *Let l be an odd prime. If i and j are arbitrary integers, then*

$$2ls(i,j) = (-1)^j D(i,l) + (-1)^{(i+j)} D(-i,l) + (1+(-1)^i)(-1)^j + \sum_{v=0}^{2l-1} D(j+iv,v). \tag{19}$$

Proof. For the proof in the case $q = p$, i.e. $\alpha = 1$ one may refer to Theorem 3 of Whiteman [11]. The same proof works for $q = p^\alpha$, $\alpha \geq 1$.

Corollary 1.

$$l(s(i,j) + s(i+l,j)) = (-1)^j + (-1)^{i+j} D(-i,l) + \sum_{v=0}^{l-1} D(j-2iv-2i, 2v+1). \tag{20}$$

P r o o f (cf. Corollary in §5 of [11]). Using Proposition 6, we get

$$l(s(i,j)+s(i+l,j)) = (-1)^j + (-1)^{i+j}D(-i,l) + \sum_{v=0}^{l-1} D(j+2iv,2v).$$

Now

$$\sum_{v=0}^{l-1} D(j+2iv,2v) = \sum_{v=0}^{l-1} D(j+2iv,2l-2v-1) = \sum_{v=0}^{l-1} D(j-2iv-2i,2v+1).$$

This proves (20).

Corollary 2.

$$\begin{aligned} 2lt(i,j) &= (-1)^i D(j,l) + (-1)^{i+j+f} D(-j,l) + (-1)^{i+f} + (-1)^{i+j} \\ &\quad + (-1)^f \sum_{u=0}^{l-1} D(i-2ju-2j,2u+1) \\ &\quad + \sum_{v=0}^{l-1} D(i+j(2v+1),2v+1). \end{aligned}$$

P r o o f. By (18) and Proposition 6, we get

$$\begin{aligned} 2lt(i,j) &= (-1)^i D(j,l) + (-1)^{(i+j)} D(-j,l) + (1+(-1)^j)(-1)^i \\ &\quad + \sum_{v=0}^{2l-1} D(i+jv,v) \quad \text{when } f \text{ is even,} \\ 2lt(i,j) &= (-1)^{i+l} D(j+l,l) + (-1)^{(i+j)} D(-j-l,l) + (1+(-1)^{j+l})(-1)^{i+l} \\ &\quad + \sum_{v=0}^{2l-1} D(i+l+(j+l)v,v) \quad \text{when } f \text{ is odd.} \end{aligned}$$

In the above summations, collect the terms with v even and v odd separately. Then (combining the cases of f even and f odd) we get

$$\begin{aligned} 2lt(i,j) &= (-1)^i D(j,l) + (-1)^{i+j+f} D(-j,l) + (-1)^{i+f} + (-1)^{i+j} \\ &\quad + (-1)^f \sum_{v=0}^{l-1} D(i+2jv,2v) + \sum_{v=0}^{l-1} D(i+j(2v+1),2v+1). \end{aligned}$$

Now, as in the proof of Corollary 1, we have

$$\sum_{v=0}^{l-1} D(i+2jv,2v) = \sum_{u=0}^{l-1} D(i-2ju-2j,2u+1).$$

This gives Corollary 2.

Using Proposition 2 and Lemma 2 we now evaluate $A_{(i,j)_{2l}}$ in terms of the coefficients of certain Jacobi sums of order l and certain Jacobi sums of order $2l$.

PROPOSITION 7. *Let*

$$J_{2l}(1,n)=\sum_{i=1}^{l-1}b_i(n)\zeta^i \quad \text{and} \quad J_l(1,n)=\sum_{i=1}^{l-1}a_i(n)\zeta^i.$$

We have

$$\begin{aligned}(21)\quad & 4l^2A_{(i,j)_{2l}}\\ &= q-3l+1+\varepsilon(i)+\varepsilon(j)+\varepsilon(i-j)+l\sum_{n=1}^{l-2}a_{in+j}(n)-\sum_{n=1}^{l-2}\sum_{k=1}^{l-1}a_k(n)\\ &\quad -\{(-1)^j+(-1)^{i+f}+(-1)^{i+j}\}\Big\{l+\sum_{k=1}^{l-1}b_k(l)+\sum_{u=0}^{l-2}\sum_{k=1}^{l-1}b_k(2u+1)\Big\}\\ &\quad +(-1)^jl\Big\{b_{\nu(-i)}(l)+\sum_{u=0}^{l-1}b_{\nu(j-2iu-2i)}(2u+1)\Big\}\\ &\quad +(-1)^{i+j}l\Big\{b_{\nu(j)}(l)+\sum_{u=0}^{l-1}b_{\nu(i+2ju+j)}(2u+1)\Big\}\\ &\quad +(-1)^{i+f}l\Big\{b_{\nu(-j)}(l)+\sum_{u=0}^{l-1}b_{\nu(i-2ju-2j)}(2u+1)\Big\},\end{aligned}$$

where $a_0(n)=b_0(n)=0$,

$$\nu(j)=\begin{cases}\Lambda(j)/2 & \text{if } j \text{ is even},\\ \Lambda(j+l)/2 & \text{if } j \text{ is odd},\end{cases}$$

$\Lambda(r)$ *being defined as the least non-negative residue of* r *modulo* $2l$, *and*

$$\varepsilon(i)=\begin{cases}0 & \text{if } l\mid i,\\ l & \text{otherwise}.\end{cases}$$

Proof. From Lemma 5 we have

$$4A_{(i,j)_{2l}}=A_{(i,j)_l}+s(i,j)+s(i+l,j)+2t(i,j).$$

Hence, using Corollaries 1 and 2 above, we get

$$\begin{aligned}4l^2A_{(i,j)_{2l}} &= l^2A_{(i,j)_l}+l(-1)^j+l(-1)^{i+f}+l(-1)^{i+j}\\ &\quad +l(-1)^{i+j}D(-i,l)+l(-1)^iD(j,l)+l(-1)^{i+j+f}D(-j,l)\\ &\quad +l\sum_{u=0}^{l-1}\{D(j-2iu-2i,2u+1)+(-1)^fD(i-2ju-2j,2u+1)\\ &\quad +D(i+j(2u+1),2u+1)\}.\end{aligned}$$

Now, using (17) we get

$$\begin{aligned}
4l^2A_{(i,j)_{2l}} &= l^2A_{(i,j)_l} + (-1)^j\Big(lb_{\nu(-i)}(l) - 1 - \sum_{k=1}^{l-1} b_k(l)\Big)\\
&\quad + (-1)^{i+j}\Big(lb_{\nu(j)}(l) - 1 - \sum_{k=1}^{l-1} b_k(l)\Big)\\
&\quad + (-1)^{i+f}\Big(lb_{\nu(-j)}(l) - 1 - \sum_{k=1}^{l-1} b_k(l)\Big)\\
&\quad + (-1)^j \sum_{u=0}^{l-1} l\Big(b_{\nu(j-2iu-2i)}(2u+1) - \sum_{k=1}^{l-1} b_k(2u+1)\Big)\\
&\quad + (-1)^{i+f} \sum_{u=0}^{l-1} l\Big(b_{\nu(i-2ju-2j)}(2u+1) - \sum_{k=1}^{l-1} b_k(2u+1)\Big)\\
&\quad + (-1)^{i+j} \sum_{u=0}^{l-1} l\Big(b_{\nu(i+2ju+j)}(2u+1) - \sum_{k=1}^{l-1} b_k(2u+1)\Big),
\end{aligned}$$

i.e.

$$\begin{aligned}
4l^2A_{(i,j)_{2l}} &= l^2A_{(i,j)_l}\\
&\quad - ((-1)^j + (-1)^{i+f} + (-1)^{i+j})\Big(1 + \sum_{k=1}^{l-1} b_k(l) + \sum_{u=0}^{l-1}\sum_{k=1}^{l-1} b_k(2u+1)\Big)\\
&\quad + (-1)^j l\Big(b_{\nu(-i)}(l) + \sum_{u=0}^{l-1} b_{\nu(j-2iu-2i)}(2u+1)\Big)\\
&\quad + (-1)^{i+j} l\Big(b_{\nu(j)}(l) + \sum_{u=0}^{l-1} b_{\nu(i+2ju+j)}(2u+1)\Big)\\
&\quad + (-1)^{i+f} l\Big(b_{\nu(-j)}(l) + \sum_{u=0}^{l-1} b_{\nu(i-2ju-2j)}(2u+1)\Big).
\end{aligned}$$

Substituting the value of $A_{(i,j)_l}$ from Proposition 4 and the value of $\sum_{k=1}^{l-1} b_k(2l-1)$ as $l-1$ we get (21).

6. The arithmetic characterization of the Jacobi sums and the determination of the cyclotomic numbers of order $2l$

THEOREM 1 (main theorem). *Let p and l be odd rational primes, $p \equiv 1 \pmod{l}$ (thus $p \equiv 1 \pmod{2l}$ also), $q = p^\alpha$, $\alpha \geq 1$. Let $q = 1 + 2lf$. Let ζ*

and ξ be fixed primitive (complex) l-th and $2l$-th roots of unity respectively. Let ζ and ξ be related by $\zeta = \xi^2$, i.e. $\xi = -\zeta^{(l+1)/2}$. Let γ be a generator of $\mathbb{F}_q^*$. Let b be a rational integer such that $b = \gamma^{(q-1)/l}$ in $\mathbb{F}_p$. Let $m = \operatorname{ind}_\gamma 2$. Let $J_l(i,j)$ and $J_{2l}(i,j)$ denote the Jacobi sums in $\mathbb{F}_q$ of order l and $2l$ (respectively) related to ζ and ξ (respectively). For $(k,l) = 1$, let σ_k denote the automorphism $\zeta \mapsto \zeta^k$ of $\mathbb{Q}(\zeta)$. For $(k,2l) = 1$, let τ_k denote the automorphism $\xi \mapsto \xi^k$ of $\mathbb{Q}(\zeta)$. Thus if k is odd then $\sigma_k = \tau_k$ and if k is even then $\sigma_k = \tau_{k+l}$. Let $\lambda(r)$ and $\Lambda(r)$ denote the least non-negative residues of r modulo l and $2l$ (resp.). Let $a_0, a_1, \ldots, a_{l-1} \in \mathbb{Z}$ and let $H = \sum_{i=0}^{l-1} a_i \zeta^i$. Consider the arithmetic conditions (or the diophantine system)

(i) $q = \sum_{i=0}^{l-1} a_i^2 - \sum_{i=0}^{l-1} a_i a_{i+1}$,
(ii) $\sum_{i=0}^{l-1} a_i a_{i+1} = \sum_{i=0}^{l-1} a_i a_{i+2} = \ldots = \sum_{i=0}^{l-1} a_i a_{i+(l-1)/2}$,
(iii) $1 + a_0 + a_1 + \ldots + a_{l-1} \equiv 0 \pmod{l}$.

Let $1 \le n \le l-2$. If $a_0, a_1, \ldots, a_{l-1}$ satisfy (i)–(iii) *together with the additional conditions*

(iv) $a_1 + 2a_2 + \ldots + (l-1)a_{l-1} \equiv 0 \pmod{l}$,
(v) $p \nmid \prod_{\lambda((n+1)k)>k} H^{\sigma_k}$,
(vi) $p \mid \overline{H} \prod_{\lambda((n+1)k)>k} (b - \zeta^{\sigma_{k^{-1}}})$, *where k^{-1} is taken* $\pmod{l}$,

then $H = J_l(1,n)$ for this γ and conversely.

Let $1 \le n \le 2l-3$ be an odd integer. If $a_0, a_1, \ldots, a_{l-1}$ satisfy (i)–(iii) *together with the additional conditions*

(iv)′ $a_1 + 2a_2 + \ldots + (l-1)a_{l-1} \equiv m(n+1) \pmod{l}$,
(v)′ $p \nmid \prod_{\Lambda((n+1)k)>k} H^{\tau_k}$,
(vi)′ $p \mid \overline{H} \prod_{\Lambda((n+1)k)>k} (b - \zeta^{\tau_{k^{-1}}})$, *where k^{-1} is taken* $\pmod{2l}$,

then $H = J_{2l}(1,n)$ for this γ and conversely.

(*In* (v)′ *and* (vi)′, *k varies over only those values which satisfy $1 \le k \le 2l-1$ and $(k,2l) = 1$.*)

Moreover, for $1 \le n \le l-2$ if $a_0, a_1, \ldots, a_{l-1}$ satisfy the conditions (i)–(vi) *and if we fix $a_0 = 0$ at the outset and write the a_i corresponding to a given n as $a_i(n)$ then we have $J_l(1,n) = \sum_{i=1}^{l-1} a_i(n)\zeta^i$ and the cyclotomic numbers of order l are given by*:

$$l^2 A_{(i,j)_l} = q - 3l + 1 + \varepsilon(i) + \varepsilon(j) + \varepsilon(i-j) + l \sum_{n=1}^{l-2} a_{in+j}(n) - \sum_{n=1}^{l-2} \sum_{k=1}^{l-1} a_k(n) \tag{22}$$

where

$$\varepsilon(i) = \begin{cases} 0 & \text{if } l \mid i, \\ l & \text{otherwise}, \end{cases}$$

and the subscripts in $a_{in+j}(n)$ are considered modulo l.

Similarly, for n odd, $1 \le n \le 2l-3$, if $a_0, a_1, \dots, a_{l-1}$ satisfy the conditions (i)–(iii) *and* (iv)′–(vi)′ *and if we fix $a_0 = 0$ at the outset and write the a_i corresponding to a given n as $b_i(n)$ then we have $J_{2l}(1,n) = \sum_{i=1}^{l-1} b_i(n)\zeta^i$ and the $4l^2$ cyclotomic numbers $A_{(i,j)_{2l}}$ are given by*

$$
\begin{aligned}
(23)\quad & 4l^2 A_{(i,j)_{2l}} \\
&= q - 3l + 1 + \varepsilon(i) + \varepsilon(j) + \varepsilon(i-j) + l\sum_{n=1}^{l-2} a_{in+j}(n) - \sum_{n=1}^{l-2}\sum_{k=1}^{l-1} a_k(n) \\
&\quad - \{(-1)^j + (-1)^{i+f} + (-1)^{i+j}\}\Big\{l + \sum_{k=0}^{l-1} b_k(l) + \sum_{u=0}^{l-2}\sum_{k=0}^{l-1} b_k(2u+1)\Big\} \\
&\quad + (-1)^j l\Big(b_{\nu(-i)}(l) + \sum_{u=0}^{l-1} b_{\nu(j-2iu-2i)}(2u+1)\Big) \\
&\quad + (-1)^{i+j} l\Big(b_{\nu(j)}(l) + \sum_{u=0}^{l-1} b_{\nu(i+2ju+j)}(2u+1)\Big) \\
&\quad + (-1)^{i+f} l\Big(b_{\nu(-j)}(l) + \sum_{u=0}^{l-1} b_{\nu(i-2ju-2j)}(2u+1)\Big)
\end{aligned}
$$

where

$$
(24)\qquad \nu(j) = \begin{cases} \Lambda(j)/2 & \text{if } j \text{ is even}, \\ \Lambda(j+l)/2 & \text{if } j \text{ is odd}. \end{cases}
$$

P r o o f. The arithmetic characterization of the Jacobi sums $J_l(1,n)$ and the formulae for $A_{(i,j)_l}$ in the statement of the above theorem form the main theorem of Katre and Rajwade proved in [6], §3. Hence we concentrate on the part relating to modulus $2l$.

If $H = J_{2l}(1,n) = J(1,n)$ then from Proposition 1(6) we get (i) and (ii). By Proposition 3, $J(1,n) \equiv -\zeta^{-m(n+1)} \pmod{(1-\zeta)^2}$, we get (iii) and (iv)′.

We next prove (v)′. Note from Proposition 2 (§4) that

$$
(H) = (J(1,n)) = \prod_{\Lambda((n+1)k)>k} (\wp^{\tau_k - 1})^{\alpha}.
$$

To prove that $p \nmid \prod_{\Lambda((n+1)k)>k} (J(1,n))^{\tau_k}$ it suffices to prove that some prime divisor of p does not divide the right hand side. In fact we shall show that

$$
\wp^{\tau-1} \nmid \prod_{\Lambda((n+1)k)>k} (J(1,n))^{\tau_n}.
$$

If not, then

$$\wp^{\tau-1} \Big| \prod_{\Lambda((n+1)k)>k} \Big\{ \prod_{\Lambda((n+1)k')>k'} (\wp^{\tau_{k'-1}})^{\alpha} \Big\}^{\tau_k}.$$

Hence, there exist k and k' satisfying $1 \le k, k' \le 2l-1$, $(k, 2l) = 1$, $(k', 2l) = 1$ such that $\Lambda((n+1)k) > k$, $\Lambda((n+1)k') > k'$ and $k^{-1}k' \equiv -1 \pmod{2l}$, i.e. $k' \equiv -k \pmod{2l}$ and so $k' = 2l - k$. This gives

$$\Lambda((n+1)k') = \Lambda(-(n+1)k) = 2l - \Lambda((n+1)k) < 2l - k = k',$$

a contradiction. This proves (v)′.

To prove (vi)′, we note that $\wp | (b - \zeta)$, hence

$$\prod_{\Lambda((n+1)k)>k} \wp^{\tau_{k-1}} \Big| \prod_{\Lambda((n+1)k)>k} (b - \zeta^{\tau_{k-1}}).$$

Now we have

$$(\overline{H}) = (H^{\tau-1}) = \prod_{\Lambda((n+1)k)>k} ((\wp^{\tau_{k-1}})^{\alpha})^{\tau-1} = \prod_{\Lambda((n+1)k)>k} ((\wp^{\tau_{-k-1}})^{\alpha}).$$

Thus $J(1, n)$ satisfies (i)–(iii) as well as (iv)′–(vi)′.

Conversely, suppose H satisfies the six conditions (i)–(iii) and (iv)′–(vi)′. Then (i) and (ii) assure that $H\overline{H} = q$. (iii) and (iv)′ assure that $H \equiv -\zeta^{-m(n+1)} \pmod{(1-\zeta)^2}$. Now by (vi)′, $p \mid \overline{H} \prod_{\Lambda((n+1)k)>k} (b - \zeta^{\tau_{k-1}})$. Taking complex conjugates and using Note 1 of §4, we get $p \mid H \prod_{\Lambda((n+1)k)<k} (b - \zeta^{\tau_{k-1}})$. But by Lemma 1 of §4,

$$\text{g.c.d.} \Big((p), \prod_{\Lambda((n+1)k)<k} (b - \zeta^{\tau_{k-1}}) \Big) = \prod_{\Lambda((n+1)k)<k} \wp^{\tau_{k-1}}.$$

So, $\prod_{\Lambda((n+1)k)>k} \wp^{\tau_{k-1}} \mid H$. Let U_n and U_n' be as in Note 2 (§4). Now by (v)′ we have $p \nmid \prod_{\Lambda((n+1)k)>k} H^{\tau_k}$. Let $\wp'$ be a prime divisor of p such that $\wp' \nmid \prod_{\Lambda((n+1)k)>k} H^{\tau_k}$. Hence for every $k \in U_n$, $\wp' \nmid H^{\tau_k}$ or equivalently $\wp'^{\tau_{k-1}} \nmid H$. As $|U_n| = (l-1)/2$, there are at least $(l-1)/2$ divisors of p which do not divide H. Hence H is divisible only by $\wp^{\tau_{k-1}}$ for every $k \in U_n$. Then as $H\overline{H} = q = p^{\alpha}$, we have $(H) = \prod_{\Lambda((n+1)k)>k} (\wp^{\tau_{k-1}})^{\alpha}$. Thus H and $J(1, n)$ both are in $\mathbb{Z}[\zeta]$, both are coprime to $1 - \zeta$, and have the same absolute value, the same congruence class $\pmod{(1-\zeta)^2}$ and the same ideal decomposition. Hence by Lemma 4 (§4), $H = J(1, n)$.

The computation of the cyclotomic numbers follows from Proposition 7. This completes the proof of the main theorem.

7. Illustration. In this section we obtain unambiguous evaluation of cyclotomic numbers of order 6 for finite fields of $q = p^{\alpha}$ elements, p a prime, $p \equiv 1 \pmod 3$. We also state (as a part of Theorem 2) the result

for the cyclotomic numbers of order 3 as obtained by Katre and Rajwade in Proposition 1, §4 of [6] (a typing mistake in their statement being corrected here; no change in their proof of the Proposition).

THEOREM 2. *Let p be a prime $\equiv 1 \pmod 3$ and let $q = p^\alpha$. Let $q = 1 + 6f$. Let γ be a generator of $\mathbb{F}_q^*$. Let $m = \operatorname{ind}_\gamma 2$. Then each of the following diophantine systems has a unique solution*:

$$\text{(I)}\quad \begin{aligned} &4q = L^2 + 27M^2, \quad L \equiv 1 \pmod 3, \quad p \nmid L, \\ &\gamma^{(q-1)/3} \equiv (L + 9M)/(L - 9M) \pmod p, \end{aligned} \tag{25}$$

$$\text{(II)}\quad \begin{aligned} &4q = E^2 + 3F^2, \quad E \equiv 1 \pmod 3, \quad F \equiv -m \pmod 3, \quad p \nmid E, \\ &\gamma^{(q-1)/3} \equiv (-E + F)/(E + F) \pmod p, \end{aligned} \tag{26}$$

$$\text{(III)}\quad \begin{aligned} &q = A^2 + 3B^2, \quad A \equiv 1 \pmod 3, \quad B \equiv -m \pmod 3, \quad p \nmid A, \\ &\gamma^{(q-1)/3} \equiv -(A + B)/(A - B) \pmod p. \end{aligned} \tag{27}$$

Let ω be a primitive complex cube root of unity in terms of which the Jacobi sums of order 3 are defined and let the Jacobi sums of order 6 be defined in terms of the primitive complex sixth root ξ of unity related to ω by $\omega = \xi^2$, i.e. $\xi = -\omega^2$. Then in terms of the unique solution (L, M) we get

$$J_3(1,1) = (L + 3M)/2 + 3M\omega. \tag{28}$$

Also, in terms of the unique solutions (E, F) and (A, B) the Jacobi sums of order 6 are determined by

$$2J_6(1,1) = (-E + F)\omega - (E + F)\omega^2, \tag{29}$$

$$J_6(1,3) = (A + B)\omega + (A - B)\omega^2. \tag{30}$$

Moreover, L, M, A, B, E, F, so uniquely determined, satisfy the following:

(a) *If $m \equiv 0 \pmod 3$ then*

$$L = E = -2A, \qquad F = 2B = 3M.$$

(b) *If $m \equiv 1 \pmod 3$ then*

$$L = A - 3B, \qquad E = A + 3B, \qquad 3M = -A - B, \qquad F = A - B. \tag{31}$$

(c) *If $m \equiv 2 \pmod 3$ then*

$$L = A + 3B, \qquad E = A - 3B, \qquad F = -A - B, \qquad 3M = A - B.$$

Thus if any one of the pairs (L, M), (E, F), (A, B) is known then the remaining can be obtained using (a), (b), (c).

The cyclotomic numbers of order 3 related to γ are determined by

$$\begin{aligned} A_{0,0} &= (q - 8 + L)/9, \\ A_{1,1} = A_{2,0} = A_{0,2} &= (2q - 4 - L - 9M)/18, \\ A_{0,1} = A_{1,0} = A_{2,2} &= (2q - 4 - L + 9M)/18, \\ A_{1,2} = A_{2,1} &= (q + 1 + L)/9. \end{aligned} \tag{32}$$

For f even, the cyclotomic numbers of order 6 *satisfy*

$$\begin{gathered} A_{i,j} = A_{j,i}, \quad A_{0,1} = A_{5,5}, \quad A_{0,2} = A_{4,4}, \quad A_{0,3} = A_{3,3}, \\ A_{0,4} = A_{2,2}, \quad A_{0,5} = A_{1,1}, \quad A_{1,2} = A_{1,5} = A_{4,5}, \\ A_{1,3} = A_{2,5} = A_{3,4}, \quad A_{1,4} = A_{2,3} = A_{3,5}. \end{gathered} \tag{33}$$

In this case (i.e. f even) the 36 *cyclotomic numbers of order* 6 *related to γ are determined in terms of A and B as in the following table*:

Table 1 (*f even*)

	$m \equiv 0 \pmod 3$	$m \equiv 1 \pmod 3$	$m \equiv 2 \pmod 3$
$36A_{0,0}$	$q-17-20A$	$q-17-8A+6B$	$q-17-8A-6B$
$36A_{0,1}$	$q-5+4A+18B$	$q-5+4A+12B$	$q-5+4A+6B$
$36A_{0,2}$	$q-5+4A+6B$	$q-5+4A-6B$	$q-5-8A$
$36A_{0,3}$	$q-5+4A$	$q-5+4A-6B$	$q-5+4A+6B$
$36A_{0,4}$	$q-5+4A-6B$	$q-5-8A$	$q-5+4A+6B$
$36A_{0,5}$	$q-5+4A-18B$	$q-5+4A-6B$	$q-5+4A-12B$
$36A_{1,2}$	$q+1-2A$	$q+1-2A-6B$	$q+1-2A+6B$
$36A_{1,3}$	$q+1-2A$	$q+1-2A-6B$	$q+1-2A-12B$
$36A_{1,4}$	$q+1-2A$	$q+1-2A+12B$	$q+1-2A+6B$
$36A_{2,4}$	$q+1-2A$	$q+1+10A+6B$	$q+1+10A-6B$

For f odd, the cyclotomic numbers of order 6 *satisfy*

$$\begin{gathered} A_{0,0} = A_{3,0} = A_{3,3}, \quad A_{0,1} = A_{2,5} = A_{4,3}, \\ A_{0,2} = A_{1,4} = A_{5,3}, \quad A_{2,1} = A_{4,5}, \\ A_{0,4} = A_{1,3} = A_{5,2}, \quad A_{0,5} = A_{2,3} = A_{4,1}, \\ A_{1,0} = A_{2,2} = A_{3,1} = A_{3,4} = A_{4,0} = A_{5,5}, \\ A_{1,1} = A_{2,0} = A_{3,2} = A_{3,5} = A_{4,4} = A_{5,0}, \\ A_{1,5} = A_{1,2} = A_{2,4} = A_{4,2} = A_{5,1} = A_{5,4}. \end{gathered} \tag{34}$$

In this case (i.e. f odd) the cyclotomic numbers of order 6 *related to γ are determined in terms of A and B as in the following table*:

Table 2 (*f odd*)

	$m \equiv 0 \pmod 3$	$m \equiv 1 \pmod 3$	$m \equiv 2 \pmod 3$
$36A_{0,0}$	$q-11-8A$	$q-11-2A$	$q-11-2A$
$36A_{0,1}$	$q-1-2A+12B$	$q+1+4A$	$q+1-2A-12B$
$36A_{0,2}$	$q+1-2A+12B$	$q+1-2A+12B$	$q+1-8A+12B$
$36A_{0,3}$	$q+1+16A$	$q+1+10A-12B$	$q+1+10A+12B$
$36A_{0,4}$	$q+1-2A-12B$	$q+1-8A-12B$	$q+1-2A-12B$
$36A_{0,5}$	$q+1-2A-12B$	$q+1-2A+12B$	$q+1+4A$
$36A_{1,0}$	$q-5+4A+6B$	$q-5-2A+6B$	$q-5+4A+6B$
$36A_{2,0}$	$q-5+4A-6B$	$q-5+4A-6B$	$q-5-2A-6B$
$36A_{1,2}$	$q+1-2A$	$q+1+4A$	$q+1+4A$
$36A_{2,1}$	$q+1-2A$	$q+1-8A-12B$	$q+1-8A+12B$

P r o o f. That the diophantine system (25) has a unique solution (L, M) and for this solution $J_3(1,1)$ and the cyclotomic numbers of order 3 corresponding to the given generator γ of $\mathbb{F}_q^*$ are given by (28) and (32) respectively has already been proved by Katre and Rajwade in §3 of [6]. The formulae $(32)_2$ and $(32)_3$ given here are in the correct form removing the typing mistake in §3 of [6], and the proof therein works perfectly.

We now take up the case of cyclotomic numbers of order 6. The relations among the cyclotomic numbers of order 6 as given in (33) and (34) are the same as the relations (7) and (8) of §2 proved for the cyclotomic numbers of order $2l$. Now all the cyclotomic numbers and Jacobi sums of order 6 are known if we know $J(1,1) = J_6(1,1)$ and $J(1,3) = J_6(1,3)$. Hence we consider the conditions (i)–(iii) and (iv)′–(vi)′ of the main theorem for $l = 3$ $(2l = 6)$ and $n = 1$ and 3.

Let $b_i \in \mathbb{Z}$ and $H = b_0 + b_1\omega + b_2\omega^2$ with $b_0 = 0$.

(i) corresponds to $q = b_1^2 - b_1b_2 + b_2^2$. (ii): no condition. (iii) corresponds to $b_1 + b_2 \equiv -1 \pmod 3$. (iv)′ corresponds to

$$b_1 - b_2 \equiv \begin{cases} -m \pmod 3 & \text{if } n = 1, \\ m \pmod 3 & \text{if } n = 3. \end{cases}$$

(v)′ of our main theorem corresponds to $p \nmid H$. Now $p \nmid H$ if and only if $p \nmid b_1$ and $p \nmid b_2$, i.e. if and only if $p \nmid b_1$ as $b_1^2 - b_1b_2 + b_2^2 = q$. (Note also that as $q = (b_1 - b_2)^2 + b_1b_2 = (b_1 + b_2)^2 - 3b_1b_2$, this is also equivalent to $p \nmid (b_1 - b_2)$ and also equivalent to $p \nmid (b_1 + b_2)$.)

(vi)′ of our main theorem corresponds to $p \mid (b_1\omega^2 + b_2\omega)(b - \omega)$, i.e. $p \mid (bb_1\omega^2 + bb_2\omega - b_1 - b_2\omega^2)$, i.e. $p \mid (-bb_1 - b_1 + b_2)$ and $p \mid (-bb_1 + bb_2 + b_2)$, i.e. $bb_1 \equiv (b_2 - b_1) \pmod p$ and $b(b_2 - b_1) \equiv -b_2 \pmod p$, i.e. $b \equiv (b_2 - b_1)/b_1 \pmod p$ and $b \equiv -b_2/(b_2 - b_1) \pmod p$. (Note that $p \nmid b_1$ and $p \nmid (b_2 - b_1)$ as seen above). However, using $b_1^2 - b_1b_2 + b_2^2 = q$, we get $(b_2 - b_1)/b_1 \equiv -b_2/(b_2 - b_1) \pmod p$; hence the above is equivalent to $b \equiv (b_2 - b_1)/b_1 \pmod p$. Also $(b_2 - b_1)/b_1 \equiv -b_1/b_2 \pmod p$; hence the above is also equivalent to $b \equiv -b_1/b_2 \pmod p$.

Thus b_1 and b_2 satisfy the above mentioned diophantine conditions for $n = 1, 3$ if and only if $H = J(1,1)$ or $J(1,3)$ respectively.

This shows that the diophantine conditions

$$\text{(IV)} \qquad \begin{cases} q = b_1^2 - b_1b_2 + b_2^2, \\ b_1 + b_2 \equiv -1 \pmod 3, \\ b_1 - b_2 \equiv \begin{cases} -m \pmod 3 & \text{if } n = 1, \\ m \pmod 3 & \text{if } n = 3, \end{cases} \\ p \nmid (b_1 + b_2) \text{ (or equivalently } p \nmid b_1 \text{ or equivalently} \\ \qquad\qquad p \nmid b_2 \text{ or equivalently } p \nmid (b_1 - b_2)), \\ \gamma^{(q-1)/3} \equiv -b_1/b_2 \pmod p \end{cases}$$

have a unique solution (b_1, b_2) in integers and for this unique solution, $J(1,n) = b_1\omega + b_2\omega^2$ $(n = 1, 3)$.

For $n = 1$ put

$$E = -(b_1 + b_2) \quad \text{and} \quad F = (b_1 - b_2) \tag{35}$$

with the inverse transformations

$$b_1 = (-E + F)/2 \quad \text{and} \quad b_2 = -(E + F)/2. \tag{36}$$

If b_1, b_2 are integers so are E and F and the condition $q = b_1^2 - b_1b_2 + b_2^2$ becomes $E^2 + 3F^2 = 4q$. Conversely, if E and F are integers such that $E^2 + 3F^2 = 4q$ then E and F are of the same parity and so b_1, b_2 are integers; moreover, $q = b_1^2 - b_1b_2 + b_2^2$.

The remaining conditions of (IV) $(n = 1)$ correspond to $E \equiv 1 \pmod 3$, $F \equiv -m \pmod 3$, $p \nmid E$ and

$$\gamma^{(q-1)/3} \equiv (-E + F)/(E + F) \pmod p.$$

We thus find that b_1, b_2 are integer solutions of (IV) $(n = 1)$ if and only if E and F as defined by (35) are integer solutions of (II), hence (II) has a unique solution (E, F) and for this solution

$$2J(1,1) = (-E + F)\omega - (E + F)\omega^2,$$

as required in (29).

Next let $n = 3$. Suppose b_1, b_2 form an integral solution of (IV) $(n = 3)$. Then $J(1,3) = b_1\omega + b_2\omega^2$. Hence by Proposition 5 we get $b_1 + b_2 = -(1 + 3D(0,3))$. Now

$$D(0,3) = \sum_{k=0}^{5} \{A_{k,-3k} - A_{k,3-3k}\},$$

i.e.

$$\begin{aligned} D(0,3) = {} & \{A_{0,0} + A_{1,3} + A_{2,0} + A_{3,3} + A_{4,0} + A_{5,3}\} \\ & - \{A_{0,3} + A_{1,0} + A_{2,3} + A_{3,0} + A_{4,3} + A_{5,0}\}. \end{aligned}$$

If f is even then $A_{0,3} = A_{3,0} = A_{3,3}$, $A_{1,3} = A_{4,3}$, $A_{2,3} = A_{5,3}$. Hence we get

$$D(0,3) = \{A_{0,0} + A_{2,0} + A_{4,0}\} - \{A_{0,3} + A_{1,0} + A_{5,0}\},$$

i.e.

$$D(0,3) \equiv \{A_{0,0} + A_{1,0} + A_{2,0} + A_{3,0} + A_{4,0} + A_{5,0}\} \pmod 2,$$

i.e. $D(0,3) \equiv f - 1 \pmod 2$. Thus for f even, $D(0,3)$ is odd.

Again if f is odd, we have $A_{0,0} = A_{3,0}$, $A_{2,0} = A_{5,0}$, $A_{1,0} = A_{4,0}$. Hence we get

$$D(0,3) = \{A_{1,3} + A_{3,3} + A_{5,3}\} - \{A_{0,3} + A_{2,3} + A_{4,3}\},$$

i.e.

$$D(0,3) \equiv \{A_{0,3} + A_{1,3} + A_{2,3} + A_{3,3} + A_{4,3} + A_{5,3}\} \pmod 2,$$

i.e. $D(0,3) \equiv f \pmod 2$. Since f is odd, $D(0,3)$ is odd.

Thus for f even as well as f odd $D(0,3)$ is odd. Hence b_1, b_2 are of the same parity. Put

$$A = (b_1 + b_2)/2 \quad \text{and} \quad B = (b_1 - b_2)/2 \tag{37}$$

with the inverse transformations

$$b_1 = (A + B) \quad \text{and} \quad b_2 = (A - B). \tag{38}$$

Thus A and B are integers as b_1, b_2 are integers of the same parity. Conversely, if A and B are integers then by (38), b_1, b_2 are also integers.

Now the conditions of (IV) ($n = 3$) correspond to $A^2 + 3B^2 = q$, $A \equiv 1 \pmod 3$, $B \equiv -m \pmod 3$, $p \nmid A$, and

$$\gamma^{(q-1)/3} \equiv -(A + B)/(A - B) \pmod p.$$

We thus find that b_1, b_2 are integer solutions of (IV) ($n = 3$) if and only if A and B as defined by (37) are integer solutions of (III). Thus (III) has a unique integer solution (A, B) and for this solution

$$J_6(1,3) = (A + B)\omega + (A - B)\omega^2,$$

as required in (30).

We note, from Lemma 3, that $J(1,1) = \omega^{-m} J(1,3)$. We also have $J_6(2,2) = J_3(1,1)$ and $J_6(1,3) = \omega^{-m} J_6(2,2) = \omega^{-m} J_3(1,1)$. Considering the different cases $m \equiv 0, 1, 2 \pmod 3$ and using (28), (29), (30), we get (a), (b), (c) of (31).

We note that $b_1(1) = (-E + F)/2$ and $b_2(1) = -(E + F)/2$. Hence using (31) we get

$$b_1(1) = \begin{cases} A + B & \text{if } m \equiv 0 \pmod 3, \\ -2B & \text{if } m \equiv 1 \pmod 3, \\ -A + B & \text{if } m \equiv 2 \pmod 3, \end{cases}$$

and

$$b_2(1) = \begin{cases} A - B & \text{if } m \equiv 0 \pmod 3, \\ -A - B & \text{if } m \equiv 1 \pmod 3, \\ -2B & \text{if } m \equiv 2 \pmod 3. \end{cases}$$

We also note that $b_1(3) = A + B$, $b_2(3) = A - B$, and $b_1(5) = b_2(5) = 1$. Moreover, $b_0(1) = b_0(3) = b_0(5) = 0$ (by our initial choice). The computation of the cyclotomic numbers now follows from our main theorem (Theorem 1). This proves Theorem 2 completely.

Using (31), the cyclotomic numbers of order 6 may also be evaluated in terms of L, M (used for cyclotomic numbers of order 3 by Gauss, Dickson etc.) or in terms of E, F.

R e m a r k. It can be shown that the part of the diophantine system in (III) above, viz.

$$q = A^2 + 3B^2, \quad A \equiv 1 \pmod 3, \quad p \nmid A, \tag{39}$$

has exactly 2 solutions of the type $(A, \pm B)$ and then the sign of B can be determined by the additional condition

$$\gamma^{(q-1)/3} \equiv -(A+B)/(A-B) \pmod{p}. \tag{40}$$

Thus the condition

$$B \equiv -m \pmod{3} \tag{41}$$

in (III) is redundant. However, the congruence $F \equiv -m \pmod 3$ in (II) is irredundant as can be seen e.g. by examining the case $q = p = 7$.

Acknowledgements. The first author thanks National Board for Higher Mathematics, India for granting a research fellowship. Thanks are also due to University of Poona, Pune and Bhaskaracharya Pratishthan, Pune for providing the necessary facilities for this work.

References

[1] B. C. Berndt and R. J. Evans, *Sums of Gauss, Eisenstein, Jacobi, Jacobsthal and Brewer*, Illinois J. Math. 23 (1979), 374–437.

[2] N. Buck and K. S. Williams, *Sequel to Muskat's evaluation of the cyclotomic numbers of order fourteen*, Carleton Mathematical Series 216, November 1985, Carleton University, Ottawa, 22 pp.

[3] L. E. Dickson, *Cyclotomy, higher congruences, and Waring's problem*, Amer. J. Math. 57 (1935), 391–424.

[4] —, *Cyclotomy and trinomial congruences*, Trans. Amer. Math. Soc. 37 (1935), 363–380.

[5] M. Hall, *Cyclotomy and characters*, in: Proc. Sympos. Pure Math. 8, Amer. Math. Soc., 1965, 31–43.

[6] S. A. Katre and A. R. Rajwade, *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.

[7] —, —, *Resolution of the sign ambiguity in the determination of the cyclotomic numbers of order 4 and the corresponding Jacobsthal sum*, Math. Scand. 60 (1987), 52–62.

[8] J. B. Muskat, *The cyclotomic numbers of order fourteen*, Acta Arith. 11 (1966), 263–279.

[9] J. C. Parnami, M. K. Agrawal and A. R. Rajwade, *Jacobi sums and cyclotomic numbers for a finite field*, ibid. 41 (1982), 1–13.

[10] T. Storer, *On the unique determination of the cyclotomic numbers for Galois fields and Galois domains*, J. Combin. Theory 2 (1967), 296–300.

[11] A. L. Whiteman, *Cyclotomic numbers of order 10*, in: Proc. Sympos. Appl. Math. 10, Amer. Math. Soc., 1960, 95–111.

[12] Y. C. Zee, *Jacobi sums of order 22*, Proc. Amer. Math. Soc. 28 (1971), 25–31.

DEPARTMENT OF MATHEMATICS
FERGUSSON COLLEGE
PUNE-411004, INDIA

DEPARTMENT OF MATHEMATICS
UNIVERSITY OF POONA
PUNE-411007, INDIA

Received on 2.7.1993
and in revised form on 5.5.1994 (2457)