Conspectus materiae tomi XLI, fasciculi 1

La revue est consacrée à la Théorie des Nombres
The journal publishes papers on the Theory of Numbers
Die Zeitschrift veröffentlicht Arbeiten aus der Zahlentheorie
Журнал посвящен теории чисел

L'adresse de la Rédaction et de l'échange	Address of the Editorial Board and of the exchange	Die Adresse der Schriftleitung und des Austausches	Адрес редакции и книгообмена

ACTA ARITHMETICA
ul. Śniadeckich 8, 00-950 Warszawa

Les auteurs sont priés d'envoyer leurs manuscrits en deux exemplaires
The authors are requested to submit papers in two copies
Die Autoren sind gebeten um Zusendung von 2 Exemplaren jeder Arbeit
Рукописи статей редакция просит предлагать в двух экземплярах

ISBN 83-01-02718-5 ISSN 0065-1036

PRINTED IN POLAND

WROCŁAWSKA DRUKARNIA NAUKOWA

ACTA ARITHMETICA
XLI (1982)

Jacobi sums and cyclotomic numbers for a finite field

by

J. C. Parnami, M. K. Agrawal and A. R. Rajwade (Chandigarh, India)

1. Introduction. Let l be an odd rational prime and p a rational prime $\equiv 1 \pmod{l}$. Let $q = p^\alpha$ and let F_q be the finite field of q elements. Write $q = ln+1$. Similar to Gauss' cyclotomic numbers we define a set of l^2 integers in this more general set up as follows.

Let γ be a generator of the cyclic group F_q^*. Define a character χ on F_q^* by $\chi(\gamma) = \zeta = e^{2\pi i/l}$ and put $\chi(0) = 0$ for convenience. For $0 \leqslant i, j \leqslant l-1$ (or rather for i, j modulo l) let A_{ij} be equal to the cardinality of X_{ij}, where $X_{ij} = \{v \in F_q \mid \chi(v) = \zeta^i,\ \chi(v+1) = \zeta^j\}$. Since $v \in X_{ij}$ if and only if $-v-1 \in X_{ji}$ if and only if $-v/(v+1) \in X_{i-j,l-j}$ if and only if $-(v+1)/v \in X_{j-i,l-i}$ (since $\chi(-1) = 1$), it follows that $A_{ij} = A_{ji} = A_{i-j,l-j} = A_{j-i,l-i} = A_{l-j,i-j} = A_{l-i,j-i}$. The $l \times l$ matrix (A_{ij}) has therefore only $l+(l-1)(l-2)/6$ unknown entries if $l > 3$ (and 4 if $l = 3$). Further the following $(l+1)/2$ relations between these A_{ij} are easy consequences of the definitions and are proved in exactly the same way as the corresponding relations are proved for the classical cyclotomic numbers of Gauss:

$$\sum_{j=0}^{l-1} A_{ij} = \begin{cases} n-1 & \text{if } i = 0, \\ n & \text{if } i = 1, 2, \ldots, (l-1)/2. \end{cases}$$

For example $A_{00}+A_{01}+\ldots+A_{0,l-1} = \mathrm{Card}\{v \mid \chi(v) = 1,\ \chi(v+1) = 0\} = (q-1)/l-1 = n-1$.

In the classical theory (i.e. for $q = p$) as soon as these l^2 constants A_{ij} are known in terms of p and the essentially unique solution of a certain set of Diophantine equations, we say that the cyclotomic problem is solved for the modulus l. Our object is to extend this to a general prime power $q = p^\alpha$. Some literature already exists about this, see for example [8], [1]. For $\alpha = 1$ the case $l = 3$ was treated by Gauss [4] while the case $\alpha = 1$, $l = 5$ was treated by Dickson [2] and $\alpha = 1$, $l = 7, 11$ by Leonard and Williams [6], [9]. We shall arrive at the relevant set of Diophantine equations (whose solutions can be obtained by a finite number of operations (trials) (as for the classical cases)) and one can then get the A_{ij} in terms of p and these solutions. We give, up to the case $l = 19$, the complete method for the calculation of the A_{ij} via the so-called Jacobi functions $J(i,j)$ (defined later). The actual calculations can be done without any theoretical difficulty after our results are proved. For the cases $a = 1$, $p = 3, 5, 7, 11$, our Diophantine systems are quite different from those of the corresponding classical cases. We give full details of the transformation connecting our system with the classical ones for $l = 3$ (Gauss) and $l = 5$ (Dickson). The cases $l = 7, 11$ (Leonard and Williams) get much more complicated to connect up and we have not done this here. Of course our Diophantine system serves equally well. Our method can be easily extended for primes > 19. We stopped at $l = 19$ because $l = 23$ onwards, the class number of $Q(e^{2\pi i/l})$ is > 1. This, however, is no hindrance to our method.

To begin with we introduce the so-called Jacobi sums $J(i,j)$ defined by

$$J(i,j) = \sum_{v\in F_q} \chi^i(v)\cdot\chi^j(v+1) \qquad (0 \leqslant i, j \leqslant l-1).$$

Then we have

$$\begin{aligned}\sum_i \sum_j J(i,j) &= \sum_v \sum_i \sum_j \chi^i(v)\cdot\chi^j(v+1) = \sum_v \sum_i \chi^i(v) \sum_j \chi^j(v+1)\\ &= \sum_v \left.\begin{cases} 0 & \text{if } v \text{ is } 0 \text{ or not an } l\text{th power}\\ l & \text{if } v \text{ is an } l\text{th power} \neq 0\end{cases}\right\} \times\\ &\qquad\qquad \times \left\{\begin{matrix} 0 & \text{if } v+1 \text{ is } 0 \text{ or not an } l\text{th power}\\ l & \text{if } v+1 \text{ is an } l\text{th power} \neq 0\end{matrix}\right\}\\ &= \sum_v \begin{cases} l^2 & \text{if } v \text{ and } v+1 \text{ are both } l\text{th powers, neither} = 0,\\ 0 & \text{otherwise}\end{cases}\\ &= l^2\cdot A_{00}.\end{aligned}$$

Similarly it may be shown that

$$\sum_i \sum_j \zeta^{-(ai+bj)}\cdot J(i,j) = l^2\cdot A_{ab}.$$

So it is sufficient to determine the $J(i,j)$ in order to get the A_{ij}. We now prove some relations amongst the J's which will help us to calculate them.

2. Properties of the $J(i,j)$. The following are almost trivial and we list them merely for completeness.

(i) $J(i,j) = J(j,i) = J(-i-j, j) = J(j, -i-j) = J(i, -i-j) = J(-i-j, i)$.

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

(iii) For $(k,l) = 1$, $\sigma_k J(i,j) = J(ik, jk)$, where σ_k is the automorphism $\zeta \to \zeta^k$ of $Q(\zeta)$ over Q.

(iv) (Stickelberger [8]). If $a+b+c \equiv 0 \pmod{l}$ then $J(a,b) = J(b,c) = J(c,a)$.

It follows that at most the following J's are to be determined: $J(1,1), J(1,2), \ldots, J\big(1, (l-1)/2\big)$ and indeed $J\big(1, (l-1)/2\big) = J\big((l-1)/2, (l-1)/2\big)$ (by (iv)) $= \sigma_{(l-1)/2} J(1,1)$. So if $l > 3$ then the number of J's to be calculated reduces to $(l-3)/2$.

We come now to some of the non-trivial properties of the J's. Write J_a to mean $J(1,a)$ for $(a,l) = 1$.

LEMMA 1.

$$J_a\cdot\bar{J}_a = \begin{cases} q & \text{if } a+1 \not\equiv 0 \pmod{l},\\ 1 & \text{if } a+1 \equiv 0 \pmod{l}\end{cases}$$

(see [5], [8], [1], [2]).

Proof. Since $(a,l) = 1$ so

$$\begin{aligned}J_a\cdot\bar{J}_a &= \sum_u \sum_v \chi(u)\bar{\chi}(v)\chi^a(u+1)\bar{\chi}^a(v+1)\\ &= \sum_{u=v} \chi(u)\bar{\chi}(v)\chi^a(u+1)\bar{\chi}^a(v+1) + \sum_{u\neq v} \chi(u)\bar{\chi}(v)\chi^a(u+1)\bar{\chi}^a(v+1)\\ &= q-2+\sum_{u\neq v} \chi(u)\bar{\chi}(v)\chi^a(u+1)\bar{\chi}^a(v+1).\end{aligned}$$

In this sum put $u = st$, $v = s$, then it is

$$\begin{aligned}&= q-2+\sum_{s,t(t\neq 1)} \chi(st)\bar{\chi}(s)\chi^a(st+1)\bar{\chi}^a(s+1)\\ &= q-2+\sum_{s,t(t\neq 1,0)} \chi(st)\bar{\chi}(s)\chi^a(st+1)\bar{\chi}^a(s+1) \qquad \text{(since for } t = 0 \text{ the term is } 0)\\ &= q-2+\sum_{t\neq 0,1} \chi(t) \sum_{s\neq 0,-1} \chi^a\big((st+1)/(s+1)\big) \qquad \text{(note that } (st+1)/(s+1) \neq t, 1\\ &\qquad\qquad \text{and } (st+1)/(s+1) = (s't+1)/(s'+1) \text{ if and only if } s = s')\\ &= q-2+\sum_{t\neq 0,1} \chi(t)\big(-\chi^a(t)-1\big)\\ &= q-2-\sum_{\text{all } t} \{\chi^{a+1}(t)+\chi(t)\}+2\\ &= q-\sum_t \chi^{a+1}(t) = \begin{cases} q & \text{if } a+1 \not\equiv 0 \pmod{l}\\ 1 & \text{if } a+1 \equiv 0 \pmod{l}.\end{cases}\end{aligned}$$

This completes the proof of Lemma 1.

LEMMA 2. *Let $p \equiv 1 \pmod{l}$ and let $b = \gamma^{(q-1)/l}$. Then $b \in F_p$. If b' is any integer such that $b' = b$ in F_p then $N_{Q(\zeta)/Q}(b'-\zeta) \equiv 0 \pmod{p}$. Further there is exactly one prime divisor $\mathfrak{p}$ of p in $\mathbf{Z}[\zeta]$ which divides $b'-\zeta$.*

Proof. $b^l = \gamma^{q-1} = 1$ and the equation $X^l = 1$ has exactly l roots in F_p since $l \mid p-1$, and so $b \in F_p$. Further

$$N_{Q(\zeta)/Q}(b'-\zeta) = (b'-\zeta)(b'-\zeta^2)\ldots(b'-\zeta^{l-1}) = (b'^l-1)/(b'-1) = 0$$

in F_p since $b' = b \neq 1$ in F_q. It follows that there is at least one prime divisor $\mathfrak{p}$ of p which divides $b'-\zeta$. If $\mathfrak{p}'$ is another one then clearly $\mathfrak{p}' = \mathfrak{p}^\sigma$ (where σ is an automorphism of $Q(\zeta)/Q$), $\sigma \neq 1$ and then $b'-\zeta \equiv 0 \pmod{\mathfrak{p}}$, $b'-\zeta = 0 \pmod{\mathfrak{p}^\sigma}$. Apply σ to the first and subtract from the second, we get $\zeta^\sigma - \zeta \equiv 0 \pmod{\mathfrak{p}^\sigma}$, i.e. $\zeta(1-\zeta^\sigma\zeta^{-1}) \equiv 0 \pmod{\mathfrak{p}^\sigma}$. Taking norms we see that $l \equiv 0 \pmod{\mathfrak{p}^\sigma}$ and so $l \equiv 0 \pmod{p}$, a contradiction. This proves Lemma 2.

LEMMA 3. *Let* $\mathfrak{p}$ *be as in Lemma* 2, *then* $J_a^{\sigma_k} \equiv 0 \pmod{\mathfrak{p}}$ *if and only if* $\lambda\big((a+1)k\big) > k$ *where* $\lambda(r)$ *is defined as the least non-negative residue of* r *modulo* l.

Proof. Consider the expression $S_k = \sum\limits_{v\in F_q} v^{k(q-1)/l}\cdot(v+1)^{ak(q-1)/l}$. This is in F_p (since each term is in F_p) and clearly $S_{k+l} = S_k$. We claim that $S_k = 0$ (in F_p) if and only if $\lambda\big((a+1)k\big) > k$. This is done as follows:

$$S_k = \sum_v (v-1)^{k(q-1)/l}\cdot v^{ak(q-1)/l} = \sum_v \sum_{j=0}^{k(q-1)/l} v^{(a+1)k(q-1)/l-j}\cdot\binom{k(q-1)/l}{j}(-1)^j$$
$$= \sum_v \sum_{j=0}^{k(q-1)/l} (-1)^j v^{b(q-1)/l-j}\cdot\binom{k(q-1)/l}{j}$$

where $b = \lambda\big((a+1)k\big)$.

Now note that

$$\sum_{v\in F_q} v^j = \begin{cases} 0 & \text{if } q-1 \nmid j,\\ q-1 & \text{otherwise.}\end{cases}$$

In the above sum $q-1 \mid$ the exponent $b(q-1)/l-j$ if and only if $j = b(q-1)/l$ since $0 \leqslant j$, $b(q-1)/l < q-1$ which cannot happen if $b > k$ because $j \leqslant k(q-1)/l$. Hence $S_k = 0$ if $b > k$. Now suppose $b \leqslant k$. Then

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

For any natural number $x < l$,

$$x(q-1)/l = (1+p+\ldots+p^{a-1})\left(\frac{p-1}{l}\cdot x\right).$$

The exact power of p dividing $\big(x(q-1)/l\big)!$ is

$$x(q-1)/l(p-1) - \frac{(p-1)}{l}\cdot x\cdot\frac{a}{(p-1)} = x(q-1)/l(p-1) - ax/l.$$

Hence the exact power of p dividing $\binom{k(q-1)/l}{b(q-1)/l}$ is

$$\big(k-b-(k-b)\big)\cdot(q-1)/l(p-1) - a\big(k-b-(k-b)\big)/l = 0.$$

Hence $S_k \neq 0$ in F_p. Now

$$J_a^{\sigma_k} - S_k = \sum\{\chi^k(v)\cdot\chi^{ak}(v+1) - v^{k(q-1)/l}\cdot(v+1)^{ak(q-1)/l}\}$$
$$= \sum\chi^k(v)\{\chi^{ak}(v+1)-(v+1)^{ak(q-1)/l}\} + \sum(v+1)^{ak(q-1)/l}\{\chi^k(v)-v^{k(q-1)/l}\}.$$

Here each term gives out a factor $b'-\zeta$ in $F_p[\zeta]$. But $S_k = 0$ in F_p if $\lambda\big((a+1)k\big) > k$ and $\neq 0$ if $\lambda\big((a+1)k\big) \leqslant k$. So $J_a^{\sigma_k} \equiv 0 \pmod{\mathfrak{p}}$ if and only if $\lambda\big((a+1)k\big) > k$. This completes the proof.

Now we write down the ideal decomposition of J_a (cf. [5], [8], [1]).

COROLLARY 1. *We have*

$$(J_a) = \prod_{\lambda((a+1)k)>k} (\mathfrak{p}^{\sigma_{k^{-1}}})^\alpha,$$

where k^{-1} *is taken* mod l.

In particular

$$(J_1) = \big(J(1,1)\big) = \prod_{1\leqslant k\leqslant(l-1)/2} (\mathfrak{p}^{\sigma_{k^{-1}}})^\alpha.$$

Proof. Immediate from Lemmas 1 and 3.

LEMMA 4. $J_a \equiv -1 \big(\bmod (1-\zeta)^2\big)$.

Remark. For $a = 1$ the lemma appears in [3] (see footnote on p. 365).

Proof.

$$J_a = \sum_{0\leqslant i,j\leqslant l-1} A_{ij}\zeta^{i+aj} = A_{00} + \sum_{j=1}^{l-1} A_{0j}(\zeta^{aj}+\zeta^j+\zeta^{-(a+1)j}) +$$
$$+ \sum_{i,j\neq 0, i\neq j} \tfrac{1}{6}A_{ij}\{\zeta^{j+ia}+\zeta^{i+ja}+\zeta^{i-(a+1)j}+\zeta^{j-(a+1)i}+\zeta^{ai-(a+1)j}+\zeta^{aj-(a+1)i}\}.$$

So $J_a-(q-2) = \sum\limits_{j=1}^{l-1}(\zeta^{aj}+\zeta^j+\zeta^{-(a+1)j}-3)A_{0j} + \sum\limits_{i,j\neq 0,\, i\neq j}\tfrac{1}{6}A_{ij}\{\zeta^{j+ia}+\ldots+ +\zeta^{aj-(a+1)i}-6\}$ (since $q-2 = \sum\limits_{\text{all } i,j} A_{ij}$) and this is congruent to $0 \big(\bmod (1-\zeta)^2\big)$ since each expression in the curly brackets is congruent to 0 modulo $(1-\zeta)^2$. Hence $J_a-(q-2) \equiv 0 \big(\bmod (1-\zeta)^2\big)$. But $l \sim (1-\zeta)^{l-1} \mid |q-1$ and so the result follows. This proof is for $l > 3$. For $l = 3$ we have

$$J_a = A_{00} + \sum_{j=1,2} A_{0j}(\omega^{aj}+\omega^j+\omega^{-(a+1)j}) + A_{12}(\omega^{1+2a}+\omega^{a+2})$$

where $\omega = e^{2\pi i/3}$. So

$$J_a-(q-2) = \sum_{j=1,2} A_{0j}(\omega^{aj}+\omega^{j}+\omega^{-(a+1)j}-3)+A_{12}(\omega^{1+2a}+\omega^{a+2}-2)$$
$$\equiv 0 \big(\mathrm{mod}\ (1-\omega)^2\big)$$

as required.

Lemma 5. *Let $\alpha, \beta \in \mathbf{Z}[\zeta]$, both prime to $(1-\zeta)$ satisfy* (i) $(\alpha) = (\beta)$, (ii) $|\alpha| = |\beta|$, (iii) $\alpha \equiv \beta \big(\mathrm{mod}\ (1-\zeta)^2\big)$, *then* $\alpha = \beta$ (cf. [7]).

Proof. By (i) $\alpha = \beta\eta$ (η a unit). By (ii) $\eta\bar{\eta} = 1$. Let $\eta = F(\zeta)$, a polynomial in ζ with rational integer coefficients. Then $F(\zeta)\cdot F(\bar{\zeta}) = 1$ and so $F(\zeta^i)\cdot F(\bar{\zeta}^i) = 1$ $(1 \leqslant i \leqslant l-1)$. Hence $|F(\zeta^i)| = 1$, i.e. $|\eta^{(i)}| = 1$. It follows that η is a root of unity. Now by (iii) $\eta \equiv 1 \big(\mathrm{mod}\ (1-\zeta)^2\big)$, hence $\eta = 1$. This completes the proof.

Corollary 2. *J is uniquely determined by the properties in the statements of Lemmas* 1, 3, 4.

Corollary 3. *All the conjugates of $J(1,1)$ are distinct.*

Proof. $\big(J(1,1)\big) = \mathfrak{p}^a_{1^{-1}}\mathfrak{p}^a_{2^{-1}}\cdots\mathfrak{p}^a_{((l-1)/2)^{-1}}$. Let $a \neq 1$ then σ_a: $\zeta \to \zeta^a$ fixes $J(1,1)$ if and only if, as sets in the field F_l,

$$\left\{a\cdot 1^{-1}, a\cdot 2^{-1}, \ldots, a\cdot\left(\frac{l-1}{2}\right)^{-1}\right\} = \left\{1^{-1}, 2^{-1}, \ldots, \left(\frac{l-1}{2}\right)^{-1}\right\},$$

i.e. if and only if

$$(*) \qquad \left\{a, 2a, \ldots, \left(\frac{l-1}{2}\right)a\right\} = \{1, 2, \ldots, (l-1)/2\}$$

(on multiplying by a^{-1} and taking inverses). This, however, cannot happen for the following reason. Let $l = \lambda a+r$ $(0 < r < a)$. Since $r < a$ so $r < \lambda a$. Thus $l < 2\lambda a$. But $l > \lambda a$, i.e. $l/2 < \lambda a < l$. Now $\lambda \leqslant (l-1)/2$ (since $a \geqslant 2$) so λa belongs to the left-hand side of $(*)$, but does not belong to the right-hand side and this is a contradiction.

Corollary 4. $J(1, m)\cdot J(1, m+1) = J(1,1)\cdot J(2, m)$; *indeed rather more generally* $J(1, m)\cdot J(m+1, n) = J(1, n)\cdot J(n+1, m)$.

Proof. First let $q = p$. Then the well known formula which writes the J's in terms of the Gauss sums, viz. $J(m, n) = G(m)\cdot G(n)/G(m+n)$ $(m, n, m+n \not\equiv 0 \ (\mathrm{mod}\ l))$ gives

$$J(1, m)\cdot J(n, m+1) = \frac{G(1)\cdot G(m)}{G(1+m)}\cdot\frac{G(n)\cdot G(m+1)}{G(m+n+1)},$$

$$J(1, n)\cdot J(n+1, m) = \frac{G(1)\cdot G(n)}{G(n+1)}\cdot\frac{G(n+1)\cdot G(m)}{G(n+m+1)}$$

and these are equal.

Now denote the J's of F_p by J_p and those of F_q by J_q. Let g (a generator of F_p^*) be taken as $\gamma^{(q-1)/(p-1)}$, where γ is a fixed generator of F_q^*. Then $\big(J_q(1, a)\big) = \big(J_p(1, a)\big)^a$ (by Corollary 1) and so $\big(J_q(a, b)\big) = \big(J_p(a, b)\big)^a$. Hence

$$\big(J_q(1, m)\cdot J_q(n, m+1)\big) = \big(J_p(1, m)\cdot J_p(n, m+1)\big)^a$$
$$= \big(J_p(1, n)\cdot J_p(n+1, m)\big)^a = \big(J_q(1, n)\cdot J_q(n+1, m)\big).$$

Thus the numbers $J_q(1, m)\cdot J_q(n, m+1)$ and $J_q(1, n)\cdot J_q(n+1, m)$ generate the same ideal and they have the same absolute value (since $|J_q(1, a)| = \sqrt{q}$ for $1 \leqslant a < l-1$). Further both are $\equiv 1 \big(\mathrm{mod}\ (1-\zeta)^2\big)$. Hence by Lemma 5 they are equal.

3. The arithmetic characterization of the J's (and so of the cyclotomic numbers).

Main Theorem. *Let a be one of $1, 2, \ldots, l-2$ (fixed). Let $H = \sum_{i \bmod l} a_i\zeta^i$ (where we may take any one of $a_i = 0$ but we leave it as it is for uniformity of our formulae). Put $X_j = \sum_{i=0}^{l-1} a_i a_{i+j}$. Suppose*

(i) $X_1 = X_2 = \ldots = X_{l-1}$,

(ii) $q = X_0 - X_1$,

(iii) $p \nmid \prod_{\lambda((a+1)k)>k} H^{\sigma_k}$,

(iv) $1+a_0+\ldots+a_{l-1} \equiv 0 \ (\mathrm{mod}\ l)$,

(v) $a_1+2a_2+\ldots+(l-1)a_{l-1} \equiv 0 \ (\mathrm{mod}\ l)$,

then H is some conjugate of $J(1, a)$ and conversely.

Proof. We first show that all these conditions are satisfied by $J(1, a)$ and all its conjugates. (i) and (ii) follow from Lemma 1, (iv) and (v) follow from Lemma 4. For (iii) we use Corollary 1 and get $J(1, a) = \prod_{\lambda((a+1)k)>k} (\mathfrak{p}^{\sigma_{k^{-1}}})^a$. Now $\mathfrak{p}^{\sigma_{-1}} \nmid$ the product on the right-hand side of (iii) for otherwise there exist k, k' satisfying $1 \leqslant k, k' \leqslant l-1$, $\lambda\big((a+1)k\big) > k$, $\lambda\big((a+1)k'\big) > k'$ and $k^{-1}k' \equiv -1 \ (\mathrm{mod}\ l)$, i.e. $k' \equiv -k \ (\mathrm{mod}\ l)$ and so $k' = l-k$ and then $\lambda\big((a+1)k'\big) = \lambda\big(-(a+1)k\big) = l-\lambda\big((a+1)k\big) < l-k = k'$ and this is a contradiction. It follows that $p \nmid$ the required product. This proves (iii) for $J(1, a)$ and so also for its conjugates.

Next by (iii), $p \nmid \prod_{\lambda((a+1)k)>k} H^{\sigma_k} = Y$ (say). By taking a suitable conjugate of H, we may suppose, without loss of generality, that $\mathfrak{p}^{\sigma_{-1}} \nmid Y$. Now let $\mathfrak{p}^{\sigma_{j^{-1}}} \mid H$, then $j^{-1}k \not\equiv -1 \ (\mathrm{mod}\ l)$ (i.e. $j \not\equiv -k \ (\mathrm{mod}\ l)$) whenever $\lambda\big((a+1)k\big) > k$. For any i, $1 \leqslant i \leqslant l-1$, exactly one of $\lambda\big((a+1)i\big) > i$ and $\lambda\big((a+1)(l-i)\big) > l-i$ holds. Hence the above j must be a k (rather than $-k$). It follows that $\mathfrak{p} \mid H$ implies $\mathfrak{p} \mid J_a$. Hence $H = J_a$ (by Lemma 1). This completes the proof of the theorem.

Remark 1. For any fixed k, $0 \leqslant k \leqslant l-1$, there exist only finitely many solutions $(x_0, x_1, \ldots, x_{l-1})$ (viz. the number of distinct conjugates of $J(1, a)$) satisfying the conditions (i)–(v) of the theorem and the extra condition $x_k = 0$. This follows since $\{\zeta^i \mid i = 0, 1, \ldots, k-1, k+1, \ldots, l-1\}$ is a basis for $Q(\zeta)$ over Q.

Remark 2. The finitely many solutions of our diophantine system ought to be computable by a finite number of trials. This can be achieved by expressing condition (ii) as a positive definite quadratic form by a change of variables. Take $a_0 = 0$. We claim that the transformation $z_j = (l-j)a_j - (a_{j+1} + \ldots + a_{l-1})$ takes (ii) (with the use of (i)) into the positive definite quadratic form

$$\frac{l-1}{2}\, q = \sum_{j=1}^{l-1} \frac{z_j^2}{2(l-j)(l-j+1)}.$$

Here $|z_j| < l^{3/2}\sqrt{q}$ and the transformation from the a_j to the z_j is non-singular. On getting the solutions in the z_j (in integers) we go back to the a_j and retain only those solutions for which the a_j are integers and satisfy (iii), (iv) and (v).

Proof. We have $\sum\limits_{i \neq j} a_i a_j = X_1 + \ldots + X_{l-1}$ (clearly) and this is equal to $(l-1)X_1$ (by (i)). Hence $\dfrac{l-1}{2}\, q = \dfrac{l-1}{2}(X_0 - X_1)$ (by (ii)) $= \dfrac{l-1}{2} X_0 - \sum\limits_{i<j} a_i a_j$ and we claim that this is equal to

$$\sum_{j=1}^{l-1} \frac{l[(l-j)a_j - (a_{j+1} + \ldots + a_{l-1})]^2}{2(l-j)(l-j+1)}.$$

This is checked by comparing coefficients as follows: The coefficient of a_i^2 is $\sum\limits_{j=1}^{i-1} l/2(l-j)(l-j+1) + l(l-i)/2(l-i+1) = (l-1)/2$ on summing by partial fractions and simplifying. The coefficient of $a_i a_j$ $(i<j)$ is $\sum\limits_{j=1}^{l-1} l/(l-j)(l-j+1) - l/(l-i+1) = -1$ as above. This completes the proof.

What remains to do now to complete the arithmetical characterization is the following: Suppose $J(1,1)$ is fixed as $\sum\limits_{i=0}^{l-1} x_i \zeta^i$ where $(x_0, \ldots, x_{l-1})$ is an arbitrary solution of the diophantine system. The conjugates of $J(1,1)$ each correspond to the remaining solutions. It then remains to fix $J(1,2)$, $J(1,3)$, $\ldots$, $J(1, (l-3)/2)$. This needs casewise handling and we now give l values $= 3, 5, 7, \ldots$ and complete this last step one by one. For the cases $l = 3$ and 5 we convert our theorem to a form similar to the classical forms in F_p due to Gauss ($l = 3$) and Dickson ($l = 5$). For the cases $l = 7$ and 11, although it is possible to get the formulation of our theorem in the Leonard–Williams form, we feel that since our diophantine system serves equally well there is no point lengthening this paper; more so as condition (iii) of our theorem becomes too complicated for the cases $l > 5$.

The case $l = 3$. Here $J(2,0) = J(0,2) = J(0,1) = J(1,0) = J(1,2) = J(2,1) = -1$ and $J(0,0) = q-2$, $J(2,2) = \bar{J}(1,1)$. So there is nothing to be done once $J(1,1)$ is fixed. By our theorem, $J(1,1) = x + y\omega$ where x, y satisfy: (i) no condition in this case, (ii) $q = p^a = x^2 + y^2 - xy$, (iii) $p \nmid x + y\omega$, (iv) $1 + x + y \equiv 0 \pmod 3$, (v) $y \equiv 0 \pmod 3$.

Now by (ii) we find that (iii) holds if and only if $p \nmid y$ and (iv) and (v) hold if and only if $y \equiv 0 \pmod 3$, $x \equiv 2 \pmod 3$. We write (ii) as $4q = (2x-y)^2 + 3y^2$ and put $y = 3V$, $2x - y = U$ and we get the following

Proposition 1. *For* $l = 3$, $J(1,1) = (U+3V)/2 + 3V\omega$, *where* $p \nmid V$, $U \equiv 1 \pmod 3$ *and* $4q = U^2 + 27V^2$.

By the remark after our main theorem it follows that the solution (U, V) of Proposition 1 has two choices where if (U, V) is one the other one is $(U, -V)$. We may, without loss of generality let $J(1,1)$ correspond to the solution (U, V) and then $J(2,2)$ will correspond to $(U, -V)$. Now we have

$$A_{00} = \tfrac{1}{9} \sum_i \sum_j J(i,j) = \tfrac{1}{9}(-6 + q - 2 + x + y\omega + x + y\omega^2) = \tfrac{1}{9}(q + U - 8),$$

$$A_{22} = A_{10} = A_{01} = \tfrac{1}{9} \sum_i \sum_j \omega^{-j} \cdot J(i,j) = \tfrac{1}{18}(2q - 4 - U + 9V),$$

$$A_{11} = A_{20} = A_{02} = \frac{q-4}{3} - \tfrac{1}{9}\left(2q - 10 + \frac{U+9V}{2}\right) = \tfrac{1}{18}(2q - 4 - U - 9V)$$

and finally

$$A_{12} = A_{21} = A_{00} + 1 = \tfrac{1}{9}(q + U + 1).$$

This gives us the cyclotomic constants. The ambiguity about the choice of $(U, \pm V)$ will, as usual, always remain as it depends on the choice of the generator γ of F_q^*. Putting $a = 1$ we get the classical theorem of Gauss [4]. Note that for the case $a = 1$, the condition $p \nmid V$ is redundant since $4p = U^2 + 27V^2$ and so $p \mid V$ implies $V = 0$ (otherwise $27V^2 > 4p$) and so $4p = U^2$ which is a contradiction. It follows that $p \nmid V$ is always true.

The case $l = 5$. Here $J(0,0) = q-2$, $J(0,1) = J(1,0) = J(0,2) = J(2,0) = J(0,3) = J(3,0) = J(0,4) = J(4,0) = J(1,4) = J(4,1) = J(2,3) = J(3,2) = -1$, $J(1,1) = J(1,3) = J(3,1) = J$ say, $J(2,1) = J(1,2) = J(2,2) = J^{\sigma_2}$, $J(3,3) = J(3,4) = J(4,3) = J^{\sigma_3}$, $J(4,4) = J(4,2) = J(2,4) = J^{\sigma_4} = \bar{J}$. So we need calculate only J. Since our aim is to get the final result in the form given by Dickson for the case $\alpha = 1$ [2] we write a conjugate of $J = a_1\zeta + a_2\zeta^2 + a_3\zeta^3 + a_4\zeta^4$, where, by our main theorem

(i) $a_1a_2 + a_2a_3 + a_3a_4 = a_1a_3 + a_2a_4 + a_4a_1$ (i.e. $B = C$ say),

(ii) $q = a_1^2 + a_2^2 + a_3^2 + a_4^2 - B$,

(iii) $p \nmid$ g.c.d. $(a_2^2 + a_1a_4 - a_1a_2 - a_2a_4 - a_1a_3,\ a_4^2 + a_2a_3 - a_1a_2 - a_2a_4 - a_3a_4,\ a_1^2 + a_2a_3 - a_1a_2 - a_1a_3 - a_3a_4,\ a_3^2 + a_1a_4 - a_2a_4 - a_1a_3 - a_3a_4)$,

(iv) $1 + a_1 + a_2 + a_3 + a_4 \equiv 0 \pmod 5$,

(v) $a_1 + 2a_2 + 3a_3 + 4a_4 \equiv 0 \pmod 5$.

Here only (iii) needs a little justification. By (iii) of the theorem $p \nmid H \cdot H^{\sigma_2}$ and

$$\begin{aligned} H \cdot H^{\sigma_2} &= (a_1\zeta + a_2\zeta^2 + a_3\zeta^3 + a_4\zeta^4)(a_1\zeta^2 + a_2\zeta^4 + a_3\zeta + a_4\zeta^3) \\ &= (a_1a_2 + a_2a_4 + a_3a_1 + a_4a_3) + \zeta(a_2^2 + a_3a_4 + a_4a_1) + \zeta^2(a_4^2 + a_1a_3 + a_2a_3) \\ &\quad + \zeta^3(a_1^2 + a_2a_3 + a_2a_4) + \zeta^4(a_3^2 + a_1a_2 + a_1a_4), \end{aligned}$$

which gives (iii) above on fixing the basis as $\zeta, \zeta^2, \zeta^3, \zeta^4$.

This could be one set of arithmetic conditions but we want one similar to Dickson's. This we now do.

By (ii), using (i) we get $q = a_1^2 + a_2^2 + a_3^2 + a_4^2 - (B+C)/2$ and after easy calculations we find $16q = X^2 + 50U^2 + 50V^2 + 125W^2$ where $X = -(a_1 + a_2 + a_3 + a_4)$, $5U = a_1 + 2a_2 - 2a_3 - a_4$ (which is $\equiv 0 \pmod 5$ by (v) and so U is an integer), $5V = 2a_1 - a_2 + a_3 - 2a_4$ (which is again $\equiv 0 \pmod 5$ on multiplying (v) by 2, and so V too is an integer), $W = a_1 - a_2 - a_3 + a_4$. Here $X \equiv 1 \pmod 5$ by (iv) and by (i) $V^2 - 4UV - U^2 = XW$ (easily checked). Finally condition (iii) is got in terms of X, U, V, W as follows. Solving for a_1, a_2, a_3, a_4 we get

$$4a_1 = -X + 2U + 4V + W, \qquad 4a_2 = -X + 4U - 2V - W,$$
$$4a_3 = -X - 4U + 2V - W, \qquad 4a_4 = -X - 2U - 4V + W$$

and a fairly simple calculation yields that (iii) is equivalent to the condition

$$\begin{aligned} p \nmid \text{g.c.d.}\,(&-X^2 + 20U^2 - 20V^2 + 5W^2 - 2XU + 6XV - 20UV - 10UW + \\ &+ 10VW, -X^2 - 20U^2 + 20V^2 + 5W^2 + 6XU + 2XV + 20UV - \\ &- 10UW - 10VW, -X^2 - 20U^2 + 20V^2 + 5W^2 - 6XU - 2XV + \\ &+ 20UV + 10UW + 10VW, -X^2 + 20U^2 - 20V^2 + 5W^2 + \\ &\qquad + 2XU - 6XV - 20UV + 10UW - 10VW). \end{aligned}$$

Now use the fact that $p \nmid (a, b, c, d)$ if and only if $p \nmid (a+d, a-d, b+c, b-c)$ and the above condition is seen to boil down to

$$p \nmid (X^2 - 5W^2,\ U^2 - V^2 - UV,\ 2XU - XV - 5VW,\ XU + 2XV - 5UW).$$

Here the second term may be taken to be equal $XW + 5UV$ in view of the relation $V^2 - 4UV - U^2 = XW$. Hence we have the following

PROPOSITION 2. *For $l = 5$,*

$$\begin{aligned} J(1,1) = {} & \tfrac{1}{4}(-X + 2U + 4V + W)\zeta + \tfrac{1}{4}(-X + 4U - 2V - W)\zeta^2 + \\ & + \tfrac{1}{4}(-X - 4U + 2V - W)\zeta^3 + \tfrac{1}{4}(-X - 2U - 4V + W)\zeta^4, \end{aligned}$$

where X, U, V, W is one of the (exactly) four solutions of the diophantine system

$$16q = X^2 + 50U^2 + 50V^2 + 125W^2, \qquad V^2 - 4UV - U^2 = XW,$$

satisfying

$$X \equiv 1 \pmod 5,$$

$$p \nmid (X^2 - 5W^2,\ XW + 5UV,\ 2XU - XV - 5VW,\ XU + 2XV - 5UW).$$

If (X, U, V, W) is one solution, the remaining 3 are $(X, -U, -V, W)$, $(X, V, -U, -W)$, $(X, -V, U, -W)$. The remaining 3 conjugates of $J(1,1)$ are got by substituting these 3 solutions in the expression for $J(1,1)$.

Just as in the case $l = 3$, we may now work out all the cyclotomic constants A_{ij}. We get the following:

$$A_{00} = \tfrac{1}{25}(q - 14 + 3X), \quad A_{01} = A_{10} = A_{44} = \tfrac{1}{100}(4q - 16 - 3X + 50V + 5W),$$
$$A_{02} = A_{20} = A_{33} = \tfrac{1}{100}(4q - 16 - 3X + 50U - 5W),$$
$$A_{03} = A_{30} = A_{22} = \tfrac{1}{100}(4q - 16 - 3X - 50U - 5W),$$
$$A_{04} = A_{40} = A_{11} = \tfrac{1}{100}(4q - 16 - 3X - 50V + 5W),$$
$$A_{12} = A_{21} = A_{43} = A_{34} = A_{14} = A_{41} = \tfrac{1}{100}(4q + 4 + 2X - 10W),$$
$$A_{13} = A_{31} = A_{32} = A_{23} = A_{24} = A_{42} = \tfrac{1}{100}(4q + 4 + 2X + 10W).$$

Putting $\alpha = 1$ we get Dickson's theorem (Theorem 8 of [2]). We claim that our condition (iii) is redundant (i.e. always satisfied) in this case. For (iii) is $p \nmid HH^{\sigma_2}$ and $p = H\bar{H}$, so if $(p) = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_4$ with $\mathfrak{p}_k = \mathfrak{p}_1^{\sigma_k}$, then $(H) =$ one of $\mathfrak{p}_1\mathfrak{p}_2, \mathfrak{p}_1\mathfrak{p}_3, \mathfrak{p}_2\mathfrak{p}_4, \mathfrak{p}_3\mathfrak{p}_4$ and then $(HH^{\sigma_2}) = \mathfrak{p}_1\mathfrak{p}_2^2\mathfrak{p}_4$, $\mathfrak{p}_1^2\mathfrak{p}_2\mathfrak{p}_3$, $\mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_4^2$, $\mathfrak{p}_1\mathfrak{p}_3^2\mathfrak{p}_4$ respectively and $(p) = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_4 \nmid$ any of these. This covers everything for the case $l = 5$.

The case $l = 7$. Fix $J(1,1)$, then we need only calculate $J(1,2)$. We have (by Corollary 4 with $m = 2$, since $J(1,3) = J(3,3)$) $J(1,2) = J(1,1) \cdot J(2,2)/J(3,3)$. But $J(2,2) = \sigma_2\big(J(1,1)\big)$ and $J(3,3)$

$= \sigma_3(J(1,1))$; so this fixes $J(1,2)$. Notice that $\sigma_2(J(1,2)) = J(2,4) = J(1,2)$ and so $J(1,2) \in Q(\sqrt{-7})$ since $o(\sigma_2) = 3$.

The case $l = 11$. We need to calculate $J(1,2)$, $J(1,3)$, $J(1,4)$. We have $J(1,3) = J(7,3) = \sigma_7(J(1,2))$, $J(1,4) = J(6,1) = \sigma_6(J(1,2))$, $J(1,1)\cdot J(2,2) = J(1,2)\cdot J(1,3)$. Now all the conjugates of $J(1,1)\times \times J(2,2)$ are distinct as is easy to check using the ideal decomposition of $J(1,1)$ given in Corollary 1. So the above relations fix everything once $J(1,1)$ is fixed.

The case $l = 13$. We need only calculate $J(1,2)$, $J(1,3)$, $J(1,4)$, $J(1,5)$. We have $J(1,4) = J(4,8) = \sigma_4(J(1,2))$, $J(1,5) = J(7,1) = \sigma_7(J(1,2))$. Further $J(1,2)\cdot J(1,3) = J(1,1)\cdot J(2,2)$. It remains to fix $J(1,2)$. Now put $m = 1$, $n = 4$ in Corollary 4; we get $J(1,1)\cdot J(2,4) = J(1,4)\cdot J(1,5)$, i.e.

$$(*)\qquad J(1,1) = \frac{\sigma_4(J(1,2))\cdot\sigma_7(J(1,2))}{\sigma_2(J(1,2))}.$$

By Lemma 3 all conjugates of $J(1,1)$ are distinct and so there is only one conjugate of $J(1,2)$ that satisfies $(*)$, which therefore fixes $J(1,2)$.

The case $l = 17$. We need to fix $J(1,2), \ldots, J(1,7)$. We have $J(1,4) = J(4,12) = \sigma_4(J(1,3))$, $J(1,5) = J(11,5) = \sigma_{11}(J(1,2))$, $J(1,6) = \sigma_6(J(1,3))$, $J(1,7) = J(9,1) = \sigma_9(J(1,2))$ and $J(1,2)\cdot J(1,3) = J(1,1)\cdot J(2,2)$. It remains to fix $J(1,2)$. Put $m = 1$, $n = 3$ in Corollary 4; we get $J(1,1) = J(1,3)\cdot\sigma_4(J(1,3))/\sigma_{12}(J(1,3))$ and as for the case $l = 13$ this fixes $J(1,3)$.

The case $l = 19$. We must fix $J(1,2), \ldots, J(1,8)$. We have $J(1,4) = J(14,4) = \sigma_{14}(J(1,3))$, $J(1,5) = J(13,1) = \sigma_{13}(J(1,3))$, $J(1,6) = J(6,12) = \sigma_6(J(1,2))$, $J(1,8) = J(10,1) = \sigma_{10}(J(1,2))$. Next put $m = 6$, $n = 4$ in Corollary 4, we get $J(1,6)\cdot J(1,7) = J(1,1)\cdot J(2,6)$, which fixes every J in terms of $J(1,2)$, $J(1,3)$. Now the usual relation $J(1,1)\cdot J(2,2) = J(1,2)\cdot J(1,3)$ gives $J(1,2)$ in terms of $J(1,3)$. Apply σ_2 to this; we get $J(2,2)\cdot J(4,4) = J(2,4)\cdot J(2,6)$ and put $m = 1$, $n = 4$ in Corollary 4; we get $J(1,1)\cdot J(2,4) = J(1,4)\cdot J(1,5)$. Now eliminate $J(2,4)$ from these two equations and we get $J(1,1)\cdot J(2,2)\times \times J(4,4) = J(1,4)\cdot J(1,5)\cdot J(2,6)$, i.e. $J(1,1)^{1+\sigma_2+\sigma_4} = J(1,3)^{\sigma_{14}+\sigma_{13}+\sigma_2}$. The usual argument now fixes $J(1,3)$. This completes the case $l = 19$.

Remark. Our condition (iii) of the main theorem is the crucial condition. For $q = p$ this condition is redundant for the cases $l = 3, 5$ but not for $l \geqslant 7$ and even for $l = 13$ it gets frightfully complicated in terms of the z_j (the variables of the positive definite quadratic form condition). Perhaps this is the reason why the cases $l = 13$ onwards had not been solved so far.

References

[1] H. Davenport und H. Hasse, *Die Nullstellen der Kongruenzzetafunctionen in gewissen Zyklischen Fällen*, Crelle 172 (1935), pp. 151–182.

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

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

[4] C. F. Gauss, *Disquisitiones Arithmeticae*, Section 358.

[5] E. Kummer, *Über die Erganzungssätze zu den allgemeinen Reziprozitätsgesetzen*, Crelle 44 (1852), pp. 106–121.

[6] P. A. Leonard and K. S. Williams, *The cyclotomic numbers of order* 11, Acta Arith. 24 (1975), pp. 365–383.

[7] — — *Evaluation of certain Jacobsthal sums*, Bullettino U.M.I. 15-B (1978), pp. 717–723.

[8] L. Stickelberger, *Über eine Verallgemeinerung der Kreisteillung*, Math. Ann. 37 (1890), pp. 321–367.

[9] K. S. Williams, *Elementary treatment of a quadratic partition of primes $p \equiv 1$* (mod 7), Illinois J. Math. 18 (1974), pp. 608–621.

MATHEMATICS DEPARTMENT
PANJAB UNIVERSITY
Chandigarh, India

Received on 6. 11. 1979
and in revised form on 27. 3. 1980 (1107)