Conspectus materiae tomi XLV, fasciculi 3

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 Austauches	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 83-01-06127-8 ISSN 0065-1036

PRINTED IN POLAND

W R O C Ł A W S K A D R U K A R N I A N A U K O W A

ACTA ARITHMETICA
XLV (1985)

Complete solution of the cyclotomic problem in F_q for any prime modulus l, $q = p^\alpha$, $p \equiv 1 \pmod l$*

by

S. A. Katre 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 $q = p^\alpha$, $\alpha \geqslant 1$, and let F_q be the finite field of q elements. Let ζ be a primitive (complex) lth root of unity fixed once for all. Given a generator γ of F_q^*, the Jacobi sums $J(i, j)$ and the cyclotomic numbers A_{ij} of order l, for $0 \leqslant i, j \leqslant l-1$ (or rather for i, j modulo l), are defined by

$$J(i, j) = \sum_{v \in F_q} \chi^i(v)\chi^j(v+1),$$

and

$$A_{ij} = \text{Card. } \{v \in F_q \mid \chi(v) = \zeta^i,\ \chi(v+1) = \zeta^j\},$$

where the character χ on F_q is defined by $\chi(\gamma) = \zeta$ and $\chi(0) = 0$. (Clearly, the A_{ij} do not depend upon ζ whereas the $J(i, j)$ do.) These are related by

$$\sum_i \sum_j \zeta^{-(ai+bj)} J(i, j) = l^2 A_{ab} \quad \text{and} \quad \sum_i \sum_j A_{ij} \zeta^{ai+bj} = J(a, b).$$

Thus knowing the Jacobi sums one knows the cyclotomic numbers and conversely. One has $J(0, 0) = q-2$, $J(0, j) = -1$ if $j \not\equiv 0 \pmod l$, $J(i, j) = J(j, i) = J(i, -i-j) = J(j, -i-j) = J(-i-j, i) = J(-i-j, j)$, and for $(k, l) = 1$, $J(i, j)^{\sigma_k} = J(ik, jk)$, where σ_k is the automorphism $\zeta \to \zeta^k$ of $Q(\zeta)$ over Q. From this one sees that all the Jacobi sums and the cyclotomic numbers of order l are known if one knows the Jacobi sums $J(1, 1), \ldots, J(1, (l-3)/2)$ for $l > 3$, and $J(1, 1)$ for $l = 3$ (see [9]). If γ and $\gamma' = \gamma^k$ are two generators of F_q^* and if $k\bar{k} \equiv 1 \bmod l$, then $J(i, j)_{\gamma'} = J(i\bar{k}, j\bar{k})_\gamma$. This shows that the conjugates of $J(i, j)$ for a given γ are the values of $J(i, j)$ for different generators γ of F_q^* and conversely.

The determination of the cyclotomic numbers of order $l = 3$ in F_p was considered by Gauss in [3] in terms of the solutions of the diophantine

* This paper was presented in the Indo-Soviet Symposium in Number Theory held at Centre for Advanced Study in Mathematics, Chandigarh, India, during January 16–21, 1984.

system $4p = L^2+27M^2$, $L \equiv 1 \pmod 3$ when he obtained his period equation in this case in terms of the uniquely determined L. (The three cyclotomic periods of order 3 satisfy $x^3+x^2-\frac{p-1}{3}x-\frac{1}{27}(3p-1+pl) = 0$.) Later, this case $l = 3$ was again taken up by Dickson in § 9 of [1] in connection with Waring's problem.) These equations determine L uniquely, but M is determined only upto sign. Gauss gives formulae for cyclotomic numbers of order 3 in terms of L and M, e.g. he proves that $A_{11} = (2p-4-L+9M)/18$. He says that these formulae give the cyclotomic numbers of order 3 for some primitive root γ of F_p. If M is replaced by $-M$ in all the formulae then one gets cyclotomic numbers corresponding to some other primitive root $\gamma' \bmod p$ (in fact γ' can be any primitive root satisfying $\operatorname{ind}_\gamma \gamma' \equiv 2 \bmod 3$). One says that the cyclotomic problem in F_p for $l = 3$ was solved by Gauss. However the solution does not make it clear which sign of M goes with which γ, without an alternative evaluation (from definition or otherwise) of some cyclotomic number of order 3, say A_{10} or A_{11}. In a footnote to the section 358 of *Disquisitiones Arithmeticae* [3] (p. 444, English edition or p. 432, German edition) Gauss remarks: "As far as the ambiguity of the sign of M in $4p = L^2+27M^2$, $L \equiv 1 \pmod 3$, for the determination of cyclotomic numbers of order 3, is concerned, it is unnecessary to consider this question here, and by the nature of the case it cannot be determined because it depends on the selection of the primitive root $g \bmod p$. For some primitive roots, M will be positive, for others negative" (see also Dickson [1], § 9).

Marshall Hall [4] and Storer [11] generalized the results of Gauss and Dickson for $l = 3$ to finite fields of $q = p^\alpha$ elements. However when $p \equiv 1 \pmod 3$, their results for F_q again have a Gauss-type ambiguity. Whiteman [14] has avoided the Gauss ambiguity for $q = p$ using Jacobsthal sums, whereas to remove this ambiguity Williams requires an additional agent π (a prime factor of p in the Eisenstein domain $Z[\omega]$, $\omega = \exp(2\pi i/3)$) (see [18] and [16], p. 278). In our Proposition 1 in § 3, we are able to resolve the sign ambiguities of Gauss–Dickson and Hall–Storer giving a condition of equality of the cube root $\gamma^{(q-1)/3}$ of unity (mod p) with the cube root of unity, viz. $(L+9M)/(L-9M)$, thus determining the sign of M and the cyclotomic numbers of order 3 without using Jacobsthal sums or the prime factor π of p.

We thank the referee for pointing out to us a paper by T. Stieltjes [10], [13] in which the sign ambiguity of M has been resolved for the case $q = p$.

More generally, the cyclotomic problem in F_p (or in F_q) is said to be solved (in the Gauss–Dickson sense) for the modulus l if the l^2 cyclotomic numbers are known in terms of solutions of certain diophantine equations. Here the cyclotomic numbers corresponding to some primitive root $\gamma \bmod p$ (in F_q, corresponding to some generator γ of F_q^*) are found and it may not be clear, to which γ the results correspond. Thus classically one tries to solve the cyclotomic problem upto primitive roots. In [3] (§ 358), Gauss

uses his theory of the cyclotomic periods to obtain the above-mentioned diophantine system and also the formulae for cyclotomic numbers for $l = 3$ in F_p. This was done around 1801. In 1935, the case $l = 3$ as well as the next case $l = 5$ were treated for $q = p$ (i.e. $\alpha = 1$) by Dickson [1] using the properties of Jacobi sums. For the case $l = 5$, Dickson considers the diophantine system $16p = x^2+50u^2+50v^2+125w^2$, $xw = v^2-4uv-u^2$, $x \equiv 1 \pmod 5$. This system has 4 solutions. If (x, u, v, w) is one solution then the remaining three are $(x, -u, -v, w)$, $(x, v, -u, -w)$ and $(x, -v, u, -w)$. In terms of these solutions Dickson gives formulae for cyclotomic numbers of order 5, e.g. $A_{00} = \frac{1}{25}(p-14+3x)$, $A_{01} = \frac{1}{100}(4p-16-3x+50v+25w)$ etc. However, Dickson does not tell which solution goes with which γ. Again Whiteman determines the solution (x, u, v, w) corresponding to γ for the determination of cyclotomic numbers of order 5, in terms of Jacobsthal sums [14]. As before Williams uses a prime factor $\mathfrak{P}$ of p in $Z[\exp(2\pi i/5)]$ to give the exact connection (see [17], p. 549). In 1982, Parnami, Agrawal and Rajwade generalized the results of Dickson for $l = 5$ in F_q, $q = p^\alpha$, $p \equiv 1 \pmod 5$. (See their Proposition 2 in [9] (a calculation error in their § 3 of [9] can be removed by replacing W by $5W$ in all the expressions except in XW and $125W^2$).) They again did not remove the sign-ambiguity of Dickson-type. In our Proposition 2 in § 3 we state a result which resolves this sign-ambiguity using a fifth root of unity mod p in terms of a solution of the corresponding diophantine system and thus avoiding the use of external agents like Jacobsthal sums of order 5 or a prime factor of p in $Z[\exp(2\pi i/5)]$ (in other words not going outside the relevant diophantine system).

Following Dickson, Leonard and Williams treated the next cases $l = 7$ (1974) [5], [6] and $l = 11$ (1975) [7] again using properties of the Jacobi sums. For $l = 7$ they solved the cyclotomic problem in the Gauss–Dickson sense and also obtained cyclotomic numbers of order 7 in terms of Jacobsthal sums. For $l = 11$, they connect the Jacobi sums with Jacobsthal–Whiteman sums, but they could not locate the Jacobi sums even upto conjugates without it, hence their solution to the cyclotomic problem in this case is somewhat incomplete.

In 1982, Parnami, Agrawal and Rajwade treated the problem for the general l-case in the setting of finite fields of $q = p^\alpha$ elements ($p \equiv 1 \pmod l$). Their results make an indispensable use of Jacobi sums. They considered a diophantine system (see conditions (i), (ii), (iii) and (iv) of the following theorem) which generalizes the diophantine systems of Gauss–Dickson and Leonard–Williams; moreover they gave a rejection condition (see condition (v) below) which fixes certain Jacobi sums upto conjugates. A slightly alternative formulation of their theorem reads as follows:

THEOREM (Parnami, Agrawal, Rajwade [9]). *Let p and l be odd rational primes, $p \equiv 1 \pmod l$, $q = p^\alpha$, $\alpha \geqslant 1$. Let ζ be a fixed primitive (complex) l-th root of unity. Let $J(i, j)$ denote the Jacobi sums of order l in F_q. For $(k, l) = 1$*

let σ_k be the automorphism $\zeta \to \zeta^k$ of $Q(\zeta)$. Let $\lambda(r)$ denote the least non-negative remainder of $r \bmod l$. Let $1 \leqslant n \leqslant l-2$ be fixed. Let $H = \sum_{i(\bmod l)} a_i \zeta^i \in \boldsymbol{Z}[\zeta]$ (where we may (or may not) give any fixed value to one of the a_i). Suppose that the a_i satisfy the arithmetic conditions (or the diophantine system):

(i) $q = \sum_{i=0}^{l-1} a_i^2 - \sum_{i=0}^{l-1} a_i a_{i+1}$, (*i.e.* $2q = (a_0-a_1)^2+(a_1-a_2)^2+ \ldots + (a_{l-2}-a_{l-1})^2+(a_{l-1}-a_0)^2$),

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

(iv) $a_1+2a_2+ \ldots +(l-1)a_{l-1} \equiv 0 \pmod l$,

(v) (*Rejection condition*) $p \nmid \prod_{\lambda((n+1)k)>k} H^{\sigma_k}$,

then $H = J(1, n)$ for some generator γ of $\boldsymbol{F}_q^*$ (in other words, given a generator γ, H is a conjugate of $J(1, n)$), and conversely. (Note that the conditions (i) and (ii) together may be written in the better looking form $2q = \sum_{i=0}^{l-1} (a_i-a_{i+j})^2$, $j = 1, 2, \ldots, (l-1)/2$.)

Using this theorem PAR show how to solve the cyclotomic problem upto a generator γ of $\boldsymbol{F}_q^*$ ($p \equiv 1 \pmod l$) for the cases $l \leqslant 19$. They indicate a method to solve the problem in $\boldsymbol{F}_q$ for general l. However the solution for the l-case is by no means complete even upto γ, because they have not given the necessary connections among $J(1, n)$ beyond $l = 19$.

To get rid of this difficulty by an alternative means we first ask the following question: Given a generator γ of $\boldsymbol{F}_q^*$, what additional arithmetic conditions should $H = \sum_{i(\bmod l)} a_i \zeta^i$ in the above theorem satisfy so that $H = J(1, n)$ for this γ. This question is answered in our main theorem by noting that $J(1, n)$ in fact depends upon $\gamma^{(q-1)/l}$ (which belongs to $\boldsymbol{F}_p$ since $p \equiv 1 \pmod l$).

Moreover our main theorem completely solves the cyclotomic problem in $\boldsymbol{F}_q$ ($p \equiv 1 \pmod l$) for all odd primes l, and that too not just upto a generator of $\boldsymbol{F}_q^*$, but in a stronger version, viz. given a generator γ the cyclotomic numbers are determined unambiguously in terms of solutions of the diophantine system consisting of the arithmetic conditions (i)–(vi) of the main theorem for $1 \leqslant n \leqslant l-2$. (In Remark 5 of § 2 it is shown that in fact it suffices to consider the solutions for only k values of n, where for $l > 3$, $k = (l+1)/6$ if $l \equiv 5 \pmod 6$ and $k = (l+5)/6$ if $l \equiv 1 \pmod 6$.) The precise statement of our main theorem is as follows:

MAIN THEOREM. *The notations being as in the above theorem, let γ be a generator of $\boldsymbol{F}_q^*$ and b be any rational integer $\equiv \gamma^{(q-1)/l} \pmod p$. Let $H = \sum_{i(\bmod l)} a_i \zeta^i$. Suppose that the a_i satisfy the above conditions* (i), (ii), (iii), (iv), *and* (v) *together with the new condition*

(vi) $p \mid \bar{H} \prod_{\lambda((n+1)k)>k} (b-\zeta^{\sigma_k \cdot k^{-1}})$, *where k^{-1} is taken* mod l.

Then $H = J(1, n)$ for this γ and conversely. (This determines all the Jacobi sum $J(i, j)$ and the cyclotomic numbers A_{ij} of order l related to γ uniquely.) Moreover, for $1 \leqslant n \leqslant l-2$, if we fix $a_0 = 0$ at the outset and write the a_i corresponding to a given n as $a_i(n)$ (i.e. we have $J(1, n) = \sum_{i=1}^{l-1} a_i(n)\zeta^i$, $a_0(n) = 0$), then the cyclotomic numbers of order l are given by

$$l^2 A_{00} = q-3l+1-\sum_{n=1}^{l-2} \sum_{k=1}^{l-1} a_k(n),$$

and

$$l^2 A_{ij} = \varepsilon(i)+\varepsilon(j)+\varepsilon(i-j)+l \sum_{n=1}^{l-2} a_{in+j}(n)+l^2 A_{00},$$

where

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

and the suffixes in $a_{in+j}(n)$ are to be considered modulo l. This gives a complete solution of the cyclotomic problem in $\boldsymbol{F}_q$ (even overcoming the usual γ-ambiguity) for an odd prime l where $q = p^\alpha$, $p \equiv 1 \pmod l$.

The cyclotomic numbers of order 2 in $\boldsymbol{F}_q$ are given by $A_{00} = (q-5)/4$, $A_{01} = A_{10} = A_{11} = (q-1)/4$ if $q \equiv 1 \pmod 4$, $A_{00} = A_{10} = A_{11} = (q-3)/4$, $A_{01} = (q+1)/4$ if $q \equiv 3 \pmod 4$. Thus the cyclotomic problem is solved completely for any prime l, in $\boldsymbol{F}_q$, $q = p^\alpha$, $p \equiv 1 \pmod l$.

We note that condition (vi) of our main theorem is very crucial and it contains a connection between the Jacobi sum and the lth root of unity mod p given by $\gamma^{(q-1)/l}$. It is our opinion that this powerful condition can be used to obtain expressions for the lth roots of unity mod p in terms of certain Jacobi sums, and these expressions can be used to write condition (vi) in an alternative form. This we illustrate in the Gauss case $l = 3$ for finite fields $\boldsymbol{F}_q$ ($p \equiv 1 \pmod 3$) where we show that condition (vi) is equivalent to equating the cube root $\gamma^{(q-1)/3}$ of unity mod p to the cube root of unity mod p, viz. $(L+9M)/(L-9M)$, obtained in terms of a solution of the Gauss system (see Proposition 1 in the example after the proof of the main theorem). This fixes the sign of M and so also the cyclotomic numbers of order 3 in terms of γ, thereby solving the cyclotomic problem completely for $l = 3$ without the γ-ambiguity. The case $l = 5$ is much more elaborate and we

consider it in a separate paper. However we would like to mention that in this case also condition (vi) can be shown to be equivalent to equating $\gamma^{(q-1)/5}$ to certain expression for fifth root of unity mod p in terms of solutions of the Dickson–PAR system in F_q, $p \equiv 1 \pmod 5$ (after removing a calculation error in the case $l = 5$ in § 3 of [9] as stated earlier). (For the exact statement of our result see Proposition 2 in § 3).)

Thus the idea of equating $\gamma^{(q-1)/l}$ to an lth root of unity mod p is contained in our condition (vi) implicitly. It would be interesting to obtain explicit results at least for say $l = 7$ and $l = 11$. Explicit results in the general l-case seem too difficult. A discussion of this will be found in Remark 3 of § 2.

We also note that when 2 is not an lth power in F_q (i.e. equivalently in F_p, since p itself is $\equiv 1 \pmod l$), for $n = 1$ in the main theorem, i.e. for the determination of $J(1, 1)$, after letting $a_0 = 0$ at the outset the condition (vi) may be replaced by a very simple condition, viz. $a_{i'}$ is odd (other a_i even, $1 \leqslant i \leqslant l-1$) where i' is chosen uniquely by $1 \leqslant i' \leqslant l-1$, $i' \equiv -2 \operatorname{ind}_\gamma 2 \pmod l$. (If we do not fix $a_0 = 0$ then we have the condition that a_i has a parity different from the remaining a_i.) This will be treated in a separate paper along with expressions for the solutions of our diophantine system (see [6] for the case $l = 11$ in F_p) in terms of Jacobsthal sums and Jacobsthal–Whiteman sums and conversely.

2. Historical survey and some remarks. In this section, to bring out the significance of our theorem in the cyclotomic problem more clearly we give a survey of the results obtained by various authors in this connection.

To solve the cyclotomic problem in F_p up to primitive roots, Gauss ($l = 3$), Dickson ($l = 5$) and Leonard and Williams ($l = 7$ and $l = 11$) considered a diophantine system which is equivalent to the arithmetic conditions (i), (ii), (iii), (iv) of our main theorem for $q = p$ case. This four-conditional system, in the p-case, (after fixing one of the a_i there) may have at most $2^{(l-1)/2}$ solutions. In the q-case ($q = p^\alpha$) it has at most $(\alpha+1)^{(l-1)/2}$ solutions, this number being the number of all possible ideals $\mathfrak{a}$ in the ring $Z[\zeta]$ which satisfy $\mathfrak{a}\bar{\mathfrak{a}} = (q)$. (That for a given ideal factor $\mathfrak{a}$ of (q) such that $\mathfrak{a}\bar{\mathfrak{a}} = (q)$ there is at most one solution $(a_0, \ldots, a_{l-1})$ satisfying $(H) = \mathfrak{a}$, where $H = \sum_{i \pmod l} a_i \zeta^i$, can be seen from Lemma 5 of [9], however whether there always exists such a solution is not clear for $l > 19$, in which case the class number of the cyclotomic field $Q(\zeta)$ is > 1. As for $l \leqslant 19$, $Z[\zeta]$ is a P. I. D. and there is a prime factor π_1 of p in $Z[\zeta]$ satisfying $\pi_1 \equiv 1 \pmod{(1-\zeta)^2}$ by Lemma 1 in [8]. Then the $(\alpha+1)^{(l-1)/2}$ algebraic integers

$$-\pi_1^{i_1} \pi_2^{i_2} \ldots \pi_{l-1}^{i_{l-1}}, \quad i_j + i_{l-j} = \alpha, \quad \pi_j = (\pi_1)_{\zeta \to \zeta^j},$$

correspond to the exactly $(\alpha+1)^{(l-1)/2}$ distinct solutions $(a_0, \ldots, a_{l-1})$ of the four-conditional system (after fixing one of the a_i)). Out of these solutions we

are interested in only those solutions which correspond to the Jacobi sums $J(i, j)$, $i, j, i+j \not\equiv 0 \pmod l$ (which also satisfy $J(i, j)\overline{J(i, j)} = q$ and $J(i, j) \equiv -1 \pmod{(1-\zeta)^2}$ (see Lemmas 1 and 3 in § 3) and thus correspond to some solutions of the above four arithmetic conditions). In fact it is sufficient to know the solutions corresponding to $J(1, 1), \ldots, J(1, l-2)$ (or even fewer than these by Remark 5 of this section). Therefore to solve the cyclotomic problem upto a generator of F_q^* we should fulfil the following requirements:

(1) Given n, $1 \leqslant n \leqslant l-2$, out of the possible $(\alpha+1)^{(l-1)/2}$ solutions ($2^{(l-1)/2}$ solutions for $q = p$) we should tell which solutions correspond to $J(1, n)$ and its conjugates (i.e. which solutions are such that they correspond to $J(1, n)$ for some generator γ of F_q^*).

(2) Knowing (1), given two different values of n, say n_1 and n_2, we should give a connection between $J(1, n_1)$ and $J(1, n_2)$. At least one should connect each $J(1, n)$ to $J(1, 1)$, so that among the solutions giving the values of $J(1, n)$ corresponding to various generators of F_q^*, we can pick up the solution which gives $J(1, n)$ so that $J(1, 1)$ and $J(1, n)$ are connected to the same γ. Thus an arbitrary choice of a solution corresponding to $J(1, 1)$ and the choice of connected $J(1, n)$ gives the Jacobi sums and the cyclotomic numbers correctly upto generators of F_q^*.

In F_q the difficulty (1) starts right from the case $l = 3$. However, for $q = p$ these difficulties did not arise in the cases $l = 3$, $l = 5$, since everything is then connected to $J(1, 1)$, and the number of conjugates of $J(1, 1)$ is 2 and 4 respectively, which is also exactly equal to the number of solutions of the relevant diophantine system. In the case $l = 7$ for $q = p$ the system has 8 solutions and everything is connected to $J(1, 1)$ and $J(1, 2)$ which have in all $6+2 = 8$ conjugates. Of the 8 solutions, Leonard and Williams term two solutions as trivial, and these are connected to $J(1, 2)$. The remaining 6 are connected to $J(1, 1)$. This fulfils the requirement (1). The requirement (2) is fulfilled by their equation $p\, J(1, 2) = J(1, 1) J(2, 2) J(4, 4)$. For $l = 11$ ($q = p$) there are 32 solutions. In this case everything is connected to $J(1, 1)$ and $J(1, 2)$ (i.e. each Jacobi sum other than $J(i, 0)$, $J(0, i)$ and $J(i, -i)$ is a conjugate of $J(1, 1)$ or $J(1, 2)$) (see [9], the case $l = 11$), and so it is sufficient to find $J(1, 1)$ and $J(1, 2)$. There are in all $10+10 = 20$ solutions corresponding to $J(1, 1)$ and $J(1, 2)$ and their conjugates. Out of the 32, two are separated as trivial and are excluded. Of the remaining 30 solutions, Leonard and Williams do not tell us how to indicate the solutions corresponding to $J(1, 1)$ and $J(1, 2)$ and their conjugates directly. Instead, they give us the expressions for $J(1, 1)$ and $J(1, 2)$ in terms of the so-called Jacobsthal–Whiteman sums $\varphi^n(a)$ of order 11, for $n = 1$ and 2 (see [7], § 5, § 6). Thus given γ, using $\varphi^n(a)$ of order 11 they are able to find the cyclotomic numbers of order 11 correctly (i.e. not just upto a primitive root) even without using the diophantine system. This is an interesting result in

itself. However, the original problem of determining the cyclotomic numbers of order 11 in terms of the solutions of the system remains unsolved in the sense that the solution does not tell us how to select the solutions corresponding to $J(1, 1)$ and $J(1, 2)$ and how to connect them, without using the external agent viz. the Jacobsthal–Whiteman sums. This and the next cases (i.e. $l \geqslant 13$) were not considered in the literature until recently Parnami, Agrawal and Rajwade [9], considered this problem in a more general set up of finite field F_q ($q = p^\alpha$, $p \equiv 1 \pmod l$). In addition to the above described conditions (i), (ii), (iii), (iv) of our main theorem, which were generally considered in some equivalent form in the previous cases, PAR introduced one more condition (condition (v) of our main theorem) which fixes $J(1, n)$ upto conjugates (or upto generators γ). Thus they overcome difficulty (1) stated above for all odd primes l. To overcome difficulty (2), they go case by case to connect the Jacobi sums $J(1, n)$ to $J(1, 1)$ and they show the connections upto $l = 19$. Thus they solve the cyclotomic problem for the cases $l \leqslant 19$ in F_q ($q = p^\alpha$, $p \equiv 1 \pmod l$). For larger l, they indicate a method to connect at least some of the Jacobi sums, however this is not enough for us. The cyclotomic problem will be solved for general l by this method only if one either gives explicit expressions connecting the other Jacobi sums to $J(1, 1)$, or at least gives an algorithm to do so.

In the present paper, to solve the cyclotomic problem in the general l-case, we choose an entirely different path. (This was in fact motivated by our solution to the $l = 3$ case, although in this paper we derive it from the main theorem.) To overcome difficulty (2), instead of connecting the Jacobi sums among themselves, we connect each of them to the chosen generator γ of F_q^* by a new condition (condition (vi) of our main theorem). The six conditions of our theorem are very natural and they fix the Jacobi sums $J(1, n)$ completely and thus given a generator γ, the cyclotomic numbers can be uniquely determined in terms of the solutions of this new system, and the cyclotomic problem has now been solved completely in a stronger version and moreover for all odd primes l, in the set up of F_q ($q = p^\alpha$, $p \equiv 1 \pmod l$). (The solution for $l = 2$ is trivial as stated already.)

Remark 1. Since conditions (i) and (ii) of our theorem may be written as $2q = \sum_{i=0}^{l-1} (a_i - a_{i+j})^2$, $j = 1, 2, \ldots, (l-1)/2$, if we fix $a_0 = 0$, it follows that $|a_i| \leqslant \sqrt{2q}$, for $j = 1, 2, \ldots, l-1$. Even then the computer takes an exhorbitant amount of time to get the solutions of the classical conditions (i), (ii), (iii), (iv). Thus the solution of the cyclotomic problem is mostly of theoretical interest. However having got these solutions (which are at most $(\alpha+1)^{(l-1)/2}$ in number) the correct selection of the solution corresponding to $J(1, n)$ is manageable by the new conditions (v) and (vi) without much difficulty. Therefore the solution is important because to obtain the l^2 cyclotomic

numbers of order l correctly, at least in theory we do not require to handle the whole model of F_q, just the knowledge of $\gamma^{(q-1)/l} \pmod p$ is sufficient.

Remark 2. From the proof of the theorem we shall observe that for $\alpha = 1$ (i.e. $q = p$ case), condition (v) is not required to determine the Jacobi sums, i.e. it follows from the remaining five arithmetic conditions.

Remark 3. For a given n, $1 \leqslant n \leqslant l-2$, condition (vi) is equivalent to a system of $l-1$ linear equations $\bmod p$ in $b, b^2, \ldots, b^{(l-1)/2}$. Suppose that the a_i occurring in these equations correspond to a solution of the first five conditions. Then these a_i give us $J(1, n)$ for some γ and then any γ to which $J(1, n)$ corresponds will give rise to a solution $b = \gamma^{(q-1)/l}$ of the above system of $l-1$ equations. Thus the system is consistent, and at most $(l-1)/2$ equations in the system are linearly independent. The coefficient matrix of the system has rank $\leqslant (l-1)/2$. In case $J(1, n)$ does not have distinct conjugates, the rank of the coefficient matrix is in fact $< (l-1)/2$, since, then, there exist at least two generators γ, γ' of F_q^* such that $\mathrm{ind}_\gamma \gamma' \not\equiv 1 \pmod l$, both of which have the same $J(1, n)$. Thus $b = \gamma^{(q-1)/l}$ and $b = \gamma'^{(q-1)/l}$ will both be (unequal) solutions $\bmod p$ of the system. (More precisely, if γ be a generator of F_q^* corresponding to $J(1, n)$, then $b = \gamma^{(q-1)/l}$ is a solution of the b-system. Let for $k \in F_l^*$, γ_k denote any generator of F_q^* such that $\mathrm{ind}_\gamma \gamma_k \equiv k \pmod l$. Then for $G_n = \mathrm{Gal}\big(Q(\zeta)/Q(J(1, n))\big)$ and $K_n = \{k \in F_l^* \mid \sigma_k \in G_n\}$ we have $k \in K_n$ if and only if $J(1, n)^{\sigma_k} = J(1, n)$, i.e. $J(1, n)^{\sigma_{k-1}} = J(1, n)$, i.e. if and only if $\gamma_k^{(q-1)/l} = \gamma^{k(q-1)/l}$ is a solution of the b-system. Thus the solutions of the b-system, which are *ipso facto* lth roots of unity $\bmod p$, form the set $U_n = \{\gamma^{k(q-1)/l} \mid k \in K_n\}$, the cardinality of this set being $|G_n| = |K_n|$. Note that if instead of the solution of the five-conditional system corresponding to $J(1, n)$ we take a solution corresponding to a conjugate $J(1, n)^{\sigma_{k'}}$ then the above set U_n becomes $U_n' = \{\gamma^{k'^{-1}k(q-1)/l} \mid k \in K_n\}$.) However, if $J(1, n)$ has distinct conjugates, then one hopes that the rank of the coefficient matrix is in fact $(l-1)/2$. (This is actually so for $l = 3$ and $l = 5$.) If this be the case, using Cramer's rule one gets an expression for $b = \gamma^{(q-1)/l}$ in terms of the a_i's, i.e. the coefficients of $J(1, n)$. (This will be a rational expression in the a_i's of degree $(l-1)/2$ in the numerator as well as in the denominator.) PAR have checked that all the conjugates of $J(1, 1)$ are distinct (see [9], Corollary 3). Thus we hope that we should get expressions for lth roots of unity $\bmod p$ in terms of the coefficients of $J(1, 1)$, and this should also happen for $J(1, n)$ whenever it has distinct conjugates. Then one can replace condition (vi) in this case by "$\gamma^{(q-1)/l} = l$th root of unity $\bmod p$ obtained in terms of a_i's". In § 3, in an example after the proof of the main theorem, we actually verify this result for the case $l = 3$. In this case we get an expression for a primitive cube root of unity in F_q, $p \equiv 1 \pmod 3$, (viz. $(L+9M)/(L-9M)$), which is well known for $q = p$. Using this we remove the ambiguity described by Gauss in this case and give correct formulae for cyclotomic numbers of order 3. The cyclotomic problem for $l = 5$ can be similarly solved completely using an

expression for fifth root of unity in F_q, which is obtained from our condition (vi) (see the statement of Proposition 2 in § 3). As stated in the introduction one may also try $l = 7,11$ etc. similarly.

Remark 3'. Indeed the authors expect that in the distinct-conjugate-case any $(l-1)/2$ equations out of the $l-1$ equations of the b-system are linearly independent. (We can prove this for $l = 3$ and $l = 5$.) In case this is so one gets many different-looking expressions congruent to the same lth root of unity mod p (viz. $\gamma^{(q-1)/l}$), any one of which may be used to resolve the γ-ambiguity.

Remark 4. The cyclotomic numbers of order l satisfy the relations $A_{ij} = A_{ji} = A_{i-j,-j} = A_{j-i,-i} = A_{-j,i-j} = A_{-i,j-i}$. Taking $i = j$, we get $A_{ii} = A_{-i,0} = A_{0,-i}$, so we get $l-1$ classes of 3 cyclotomic numbers each. A_{00} forms a single class. For $l = 3$, $A_{12} = A_{21}$. For $l > 3$, the remaining cyclotomic numbers fall into $(l-1)(l-2)/6$ classes of 6 numbers each. Thus for $l = 3$ we need find just 4 cyclotomic numbers, whereas for $l > 3$ we need find only $(l+1)(l+2)/6$, choosing one from each class. If we use the $(l+1)/2$ additional relations (which are independent of each other and also independent of the previous ones), given by

$$\sum_{j=0}^{l-1} A_{ij} = \begin{cases} f-1 & \text{if} \quad i = 0, \\ f & \text{if} \quad 1 \leqslant i \leqslant l-1 \end{cases}$$

($q = 1+lf$), for $0 \leqslant i \leqslant (l-1)/2$, then for $l > 3$ we are left with the determination of just $(l^2-1)/6$ cyclotomic numbers of order l.

Remark 5. Consider $J(1, n)$ for $1 \leqslant n \leqslant l-2$. One has $J(1, n) = J(1, l-1-n) = \sigma_n J(1, n^{-1}) = \sigma_n J(1, l-1-n^{-1}) = \sigma_{(l-1-n)} J(1, (l-1-n)^{-1}) = \sigma_{(l-1-n)} J(1, l-1-(l-1-n)^{-1})$. For $l = 3$, it is enough to calculate $J(1, 1)$ to find the cyclotomic numbers. For $l > 3$, taking $n = 1$ we get $J(1, 1) = J(1, l-2) = J(1, (l-1)/2)$. The remaining $J(1, n)$ fall in classes of conjugates, each class corresponding to six distinct values of n, unless $n^2+n+1 \equiv 0 \pmod l$, i.e. $(2n+1)^2 \equiv -3 \pmod l$, which happens if and only if $l \equiv 1 \pmod 3$. This shows that it is sufficient to find only k $J(1, n)$, i.e. sufficient to determine solutions to our system corresponding to only k values of n, $1 \leqslant n \leqslant l-2$, where $k = (l+1)/6$ if $l \equiv 5 \pmod 6$ and $k = (l+5)/6$ if $l \equiv 1 \pmod 6$. (For $q = p$, see Dickson, [2], p. 368.)

Remark 6. For $l \equiv 1 \pmod 3$, $J(1, n)$, $n^2+n+1 \equiv 0 \pmod l$, is invariant under the automorphism $\zeta \to \zeta^n$ of order 3. Hence only $(l-1)/3$ a_i in $J(1, n)$ are independent. Thus in this case, all the cyclotomic numbers are obtained as linear combinations of in all $\frac{l-1}{6} \cdot (l-1) + \frac{l-1}{3} = (l^2-1)/6$ total number of a_i. For $l \equiv 5 \pmod 6$ one requires $\frac{1}{6}(l+1)(l-1) = (l^2-1)/6$ a_i's. In any case one obtains the cyclotomic numbers in terms of in all $(l^2-1)/6$ a_i's. Note that by Remark 4, this number is the same as the number $(l^2-1)/6$ of undetermined cyclotomic numbers. It would be interesting to see if one can lessen either or both of these numbers. (One does not have a sharper result in the literature at least upto $l = 11$.)

Remark 7. H. S. Vandiver [12] has in essence shown that for $c_i \in F_q$, $q = p^\alpha$, and for $1 \leqslant m_i \leqslant q-1$ (trivial modifications if m_i are any integers), the number of solutions of the equation $c_1 x_1^{m_1} + \ldots + c_s x^{m_s} + c_{s+1} = 0$ in F_q, can be obtained by a step by step procedure in terms of cyclotomic numbers of order e where $e = \text{g.c.d.}(q-1, \text{l.c.m.}(m_1, \ldots, m_s))$ (provided a table of indices for F_q is known). Thus in the case $e = l$, one should know the cyclotomic numbers in F_q, $q \equiv 1 \pmod l$, where p is not necessarily $\equiv 1 \pmod l$. Thus one should solve the cyclotomic problem for l in this most general case also. This has not been done by the present authors.

3. Technical lemmas, Dickson–Hurwitz sums and proof of the main theorem. In the proof of our main theorem we require the following lemmas.

LEMMA 1.

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

LEMMA 2. *Let $p \equiv 1 \pmod l$ and let $b = \gamma^{(q-1)/l}$. Then $b \in F_p$. If by abuse of notation b denotes any integer $\equiv \gamma^{(q-1)/l}$ in F_p, then $N_{Q(\zeta)/Q}(b-\zeta) \equiv 0 \pmod p$. (Here N stands for the norm.) Further there is exactly one prime divisor $\mathfrak{p}$ of p in $Z[\zeta]$ which divides $b-\zeta$, and for this $\mathfrak{p}$,*

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

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

LEMMA 3. $J(1, n) \equiv -1 \pmod{(1-\zeta)^2}$.

LEMMA 4. *$J(1, n)$ is uniquely determined by the statements of lemmas* 1, 2, 3.

(For proofs of these lemmas one is referred to [9].)

We next consider the Dickson–Hurwitz sums of order l in F_q ($q = 1+lf$). These are defined, for $i, j \bmod l$, by

$$B(i, j) = \sum_{h=0}^{l-1} (h, i-jh).$$

They satisfy the relations:

$$B(i, j) = B(i, l-1-j), \quad B(0, 0) = f-1, \quad B(i, 0) = f \quad \text{if} \quad 1 \leqslant i \leqslant l-1,$$

$$\sum_{i=0}^{l-1} B(i, j) = q-2,$$

and for $(j, l) = 1$,

$$B(i\bar{j}, \bar{j}) = B(i, j) \quad \text{where} \quad j\bar{j} \equiv 1 \pmod{l}.$$

One also has

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

$B(i, n)$ of order l may alternatively be defined by this property together with $\sum_{i=0}^{l-1} B(i, n) = q-2$. The cyclotomic numbers of order l can be given in terms of Dickson–Hurwitz sums by the formula

$$l^2 A_{ij} = -(l-1)(q-1)+\varepsilon(i)+l\sum_{n=0}^{l-1} B(in+j, n),$$

where

$$\varepsilon(i) = 0 \text{ if } l \mid i \quad \text{and} \quad \varepsilon(i) = l \text{ if } l \nmid i.$$

A proof of these results for $q = p$ is found in a paper of A. L. Whiteman (see [15]). The same reasoning works also in the F_q case. Using this result we prove the following:

LEMMA 5. *Let* $J(1, n) = \sum_{i=1}^{l-1} a_i(n)\zeta^i$. *Then the Dickson–Hurwitz sums and the cyclotomic numbers of order* l *are given by*

$$lB(i, n) = la_i(n)+(q-2)-\sum_{j=1}^{l-1} a_j(n)$$

and

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

where

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

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

In particular,

$$l^2 A_{00} = q-3l+1-\sum_{n=1}^{l-2}\sum_{k=1}^{l-1} a_k(n)$$

and

$$l^2 A_{ij} = \varepsilon(i)+\varepsilon(j)+\varepsilon(i-j)+l\sum_{n=1}^{l-2} a_{in+j}(n)+l^2 A_{00}.$$

(The formula for A_{00} has been stated by Dickson for $q = p$ on p. 370 in [2].)

Proof.

$$J(1, n) = \sum_{i=1}^{l-1} a_i(n)\zeta^i = \sum_{i=0}^{l-1} B(i, n)\zeta^i, \quad a_0(n) = 0,$$

gives

$$a_i(n) = B(i, n)-B(0, n), \quad 0 \leqslant i \leqslant l-1, \ 0 \leqslant n \leqslant l-1.$$

Summing from $i = 0$ to $l-1$ we get

$$\sum_{i=1}^{l-1} a_i(n) = q-2-lB(0, n).$$

Thus

$$lB(0, n) = q-2-\sum_{i=1}^{l-1} a_i(n).$$

This gives

$$lB(i, n) = la_i(n)+lB(0, n) = la_i(n)+(q-2)-\sum_{j=1}^{l-1} a_j(n),$$

as required.

Now

$$\begin{aligned} l^2 A_{ij} &= -(l-1)(q-1)+\varepsilon(i)+l\sum_{n=0}^{l-1} B(in+j, n) \\ &= -(l-1)(q-1)+\varepsilon(i)+\sum_{n=0}^{l-1}\{la_{in+j}(n)+(q-2)-\sum_{k=1}^{l-1} a_k(n)\} \\ &= q-1-l+\varepsilon(i)+l\sum_{n=0}^{l-1} a_{in+j}(n)-\sum_{n=0}^{l-1}\sum_{k=1}^{l-1} a_k(n). \end{aligned}$$

But $J(1, 0) = -1 = \sum_{k=1}^{l-1} a_k(0)\zeta^k$, giving $\sum_{k=1}^{l-1} a_k(0) = l-1$. Similarly $\sum_{k=1}^{l-1} a_k(l-1) = l-1$. (Note that $J(1, l-1) = -1$.)

Also

$$a_j(0) = \text{coefficient of } \zeta^i \text{ in } 'J(1, 0) = \sum_{k=1}^{l-1} \zeta^k,$$

$$= \begin{cases} 0 & \text{if } l \mid j, \\ 1 & \text{if } l \nmid j. \end{cases}$$

Thus $la_j(0) = \varepsilon(j)$. Similarly $la_{i(l-1)+j}(l-1) = \varepsilon(i-j)$. Hence

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

This proves the lemma.

We are now in a position to give

Proof of the main theorem. (I) We first show that for $H = J(1, n)$ all the six conditions are satisfied. For $0 \leqslant j \leqslant l-1$, put $X_j = \sum_{i=0}^{l-1} a_i a_{i+j}$. (Note that $X_j = X_{l-j}$ for $1 \leqslant j \leqslant l-1$.) Then using $H = \sum_{i(\mathrm{mod}\, l)} a_i \zeta^i$, one checks at once that

$$H\bar{H} = (X_0 - X_1)+(X_2-X_1)\zeta^2+ \ldots +(X_{l-1}-X_1)\zeta^{l-1}.$$

Since $H = J(1, n)$, (i) and (ii) follow from Lemma 1 and (iii) and (iv) follow from Lemma 3. To prove (v) and (vi) we use Lemma 2. For convenience let

$$S = \{k \mid 1 \leqslant k \leqslant l-1,\ \lambda((n+1)k) > k\} \quad \text{and} \quad S' = \{1, 2, \ldots, l-1\} \setminus S.$$

By Lemma 2, $(H) = \prod_{k\in S} (\mathfrak{p}^{\sigma_k - 1})^{\alpha}$. Now $\mathfrak{p}^{\sigma-1} \nmid$ the product on the right hand side of (v), for otherwise there exist $k, k' \in S$ such that $-1 \equiv k^{-1}k' (\mathrm{mod}\, l)$, i.e. $k' \equiv -k (\mathrm{mod}\, l)$. This is impossible, since for $1 \leqslant k \leqslant l-1$, $k \in S$ if and only if $l-k \notin S$. It follows that $p \nmid$ the required product. This proves (v). Next, by the choice of $\mathfrak{p}$, $\mathfrak{p} \mid (b-\zeta)$. Hence

$$\prod_{k\in S} \mathfrak{p}^{\sigma_k - 1} \Big| \prod_{k\in S} (b-\zeta^{\sigma_k - 1}).$$

Now $(p) = \prod_{1\leqslant k\leqslant l-1} \mathfrak{p}^{\sigma_k - 1}$ and $(\bar{H}) = (H)^{\sigma-1} = \prod_{k\in S'} (\mathfrak{p}^{\sigma_k - 1})^{\alpha}$ give us (vi).

(II) Conversely suppose that H satisfies the six conditions. (i) and (ii) ensure that $H\bar{H} = q$. (iii) and (iv) ensure that $H \equiv -1 (\mathrm{mod}\, (1-\zeta)^2)$. Now by (vi) $p \mid \bar{H} \prod_{k\in S} (b-\zeta^{\sigma_k - 1})$. Taking complex conjugates, $p \mid H \prod_{k\in S'} (b-\zeta^{\sigma_k - 1})$. But

$$\text{g.c.d.}\ \Big((p), \prod_{k\in S'} (b-\zeta^{\sigma_k - 1})\Big) = \prod_{k\in S'} \mathfrak{p}^{\sigma_k - 1}.$$

So, $\prod_{k\in S} \mathfrak{p}^{\sigma_k - 1} \mid H$. When $\alpha = 1$, this itself proves that $(H) = \prod_{k\in S} \mathfrak{p}^{\sigma_k - 1}$, and by Lemma 4, we get $H = J(1, n)$. However for $\alpha > 1$, we must use (v). Thus for $\alpha \geqslant 1$, by (v), $p \nmid \prod_{k\in S} H^{\sigma_k}$. Hence there exists a prime divisor $\mathfrak{p}'$ of p such that $\mathfrak{p}' \nmid \prod_{k\in S} H^{\sigma_k}$, i.e. $\mathfrak{p}' \nmid H^{\sigma_k}$ for each $k \in S$, i.e. $\mathfrak{p}'^{\sigma_k - 1} \nmid H$ for $k \in S$. This shows that there are at least $(l-1)/2 = \mathrm{card}\, S$ divisors of p which do not divide H.

Hence H is divisible only by $\mathfrak{p}^{\sigma_k - 1}$, $k \in S$. Then the condition $H\bar{H} = q$ demands that $(H) = \prod_{k\in S} (\mathfrak{p}^{\sigma_k - 1})^{\alpha}$. Hence $H = J(1, n)$ by Lemma 4.

The derivation of the formulae for cyclotomic numbers in terms of the coefficients of $J(1, n)$, i.e. in terms of the solutions of the system follows from Lemma 5. This proves the theorem.

Examples. We illustrate the ideas of the main theorem for the case $l = 3$ in the following proposition in which we resolve the sign ambiguity described by Gauss in [3] (§ 358, footnote).

PROPOSITION 1. *Let $p \equiv 1 (\mathrm{mod}\, 3)$, $q = p^{\alpha}$, and let γ be a generator of F_q^*. Let ω be the primitive cube-root of unity in terms of which we define the Jacobi sums of order 3. Then the diophantine system*

$$4q = L^2+27M^2,$$

$$p \nmid L, \quad L \equiv 1 (\mathrm{mod}\, 3),$$

$$\gamma^{(q-1)/3} \equiv (L+9M)/(L-9M) (\mathrm{mod}\, p),$$

has a unique solution (L, M) for which $J(1, 1) = (L+3M)/2+3M\omega$. Conversely, for this value of $J(1, 1)$, L, M form the unique solution of the above diophantine system. In any case, the cyclotomic numbers of order 3 related to γ are uniquely given by

$$A = A_{00} = (q-8+L)/9,$$

$$B = A_{11} = A_{20} = A_{02} = (2q-4-L+9M)/18,$$

$$C = A_{01} = A_{10} = A_{22} = (2q-4-L-9M)/18,$$

$$D = A_{12} = A_{21} = (q+1+L)/9.$$

This solves the cyclotomic problem in this case completely (without the γ-ambiguity).

Proof. Let $b = \gamma^{(q-1)/3}$. From the work of PAR (see [9], Proposition 1 and its proof) it follows that if L, M satisfy $4q = L^2+27M^2$, $p \nmid L$, $L \equiv 1 (\mathrm{mod}\, 3)$, then $J(1, 1)$ is a conjugate of $H = (L+3M)/2+3M\omega$ and conversely. Our condition (vi) may be written as

$$p \mid \bar{H}(b-\omega),$$

i.e.

$$p \mid (b-\omega)((L-3M)/2-3M\omega),$$

i.e.

$$p \mid \{b(L-3M)/2-\omega((L-3M)/2+3bM)+3M\omega^2\},$$

i.e.

$$p \mid \{(b(L-3M)/2-3M)-\omega((L+3M)/2+3bM)\},$$

i.e.

$$b(L-3M)/2-3M \equiv 0 \pmod p,$$

$$(L+3M)/2+3bM \equiv 0 \pmod p.$$

This is a system of two linear equations in b which are linearly dependent mod p. The second equation is a nonzero multiple (mod p) of the first (use $4q = L^2+27M^2$, $p \nmid L$), and conversely. From the second equation we get

$$b \equiv (L+3M)/(-6M) \pmod p \equiv (L+9M)/(L-9M) \pmod p.$$

(Note that $L+9M$, $L-9M \not\equiv 0 \pmod p$.)

This condition together with the previous conditions, fixes $J(1, 1) = (L+3M)/2+3M\omega$, and conversely, as required. The evaluation of the cyclotomic numbers can then be done as in [9]. Alternatively, from our main theorem,

$$9A_{00} = q-8-\{a_1(1)+a_2(1)\},$$

and

$$9A_{ij} = \varepsilon(i)+\varepsilon(j)+\varepsilon(i-j)+3a_{i+j}(1)+9A_{00}.$$

From this also we can get the cyclotomic numbers noting that here $a_0(1) = 0$, $a_1(1) = (-L+3M)/2$, $a_2(1) = -(L+3M)/2$. This proves the proposition. Now there is no ambiguity in the sign of M as was there in the classical case of Gauss, and the cyclotomic numbers of order 3 corresponding to a given generator γ are determined uniquely.

Remark. Note also that $(L+9M)/(L-9M)$ is a primitive cube-root of unity mod p. The other primitive cube-root of unity can be obtained by changing the sign of M. For $q = p$, this is a well-known result.

As an additional example we state here the corresponding beautiful result for $l = 5$. As said earlier, the proof is much more elaborate and will be treated in a separate paper.

PROPOSITION 2. *Let $p \equiv 1 \pmod 5$, $q = p^\alpha$, and let γ be a generator of $\mathbf{F}_q^*$. Let ζ be the primitive fifth root of unity in terms of which we define the Jacobi sums of order 5. Then the diophantine system*

$$16q = X^2+50U^2+50V^2+125W^2,$$

$$XW = V^2-4UV-U^2, \quad X \equiv 1 \pmod 5, \quad p \nmid (X^2-125W^2),$$

$$\gamma^{(q-1)/5} \equiv (A-10B)/(A+10B) \pmod p,$$

$$A = X^2-125W^2, \quad B = 2XU-XV-25VW,$$

has a unique solution (X, U, V, W). For this solution

$$J(1, 1) = \tfrac{1}{4}(-X+2U+4V+5W)\zeta+\tfrac{1}{4}(-X+4U-2V-5W)\zeta^2+$$
$$+\tfrac{1}{4}(-X-4U+2V-5W)\zeta^3+\tfrac{1}{4}(-X-2U-4V+5W)\zeta^4.$$

Conversely, for this value of $J(1, 1)$, X, U, V, W give the unique solution of the above system. In any case the cyclotomic numbers of order 5 related to γ are uniquely given by $A_{00} = \frac{1}{25}(q-14+3X)$, $A_{01} = A_{10} = A_{44} = \frac{1}{100}(4q-16-3X+50V+25W)$, etc. This solves the cyclotomic problem for $l = 5$ in this situation completely (without the usual γ-ambiguity).

References

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

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

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

[4] M. Hall, Jr., *Characters and cyclotomy*, Amer. Math. Soc. Proc. Symp. Pure Math. 8 (1965), pp. 31–43.

[5] P. A. Leonard and K. S. Williams, *A diophantine system of Dickson*, Rend. Accad. Naz. Lincei 56 (1974), pp. 145–150.

[6] – – *The cyclotomic numbers of order seven*, Proc. Amer. Math. Soc. 51 (1975), pp. 295–300.

[7] – – *The cyclotomic number of order eleven*, Acta Arith. 26 (1975), pp. 365–383.

[8] – – *Evaluation of certain Jacobsthal sums*, Bolletino U. M. I. (5) 15-B (1978), pp. 717–723.

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

[10] T. Stieltjes, *Contribution à la théorie des résidues cubiques et biquadratiques* (1883), *Oeuvres complètes*, vol. 1, Groningen 1914, pp. 210–275.

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

[12] H. S. Vandiver, *On the number of solutions of some general types of equations in a finite field*, Proc. Nat. Acad. Sci. 32 (1946), pp. 47–52.

[13] B. A. Venkov, *Elementary theory of numbers*, Groningen 1970, p. 92.

[14] A. L. Whiteman, *Cyclotomy and Jacobsthal sums*, Amer. J. Math. 74 (1952), pp. 89–99.

[15] – *The cyclotomic numbers of order ten*, Proc. Symp. Appl. Math. 10 (1960), pp. 95–111.

[16] K. S. Williams, *On Euler's criterion for cubic non-residues*, Proc. Amer. Math. Soc. 49 (1975), pp. 277–283.

[17] – *On Euler's criteria for quintic non-residues*, Pacific J. Math. 61 (1975), pp. 543–550.

[18] – *Note on the supplement to the law of cubic reciprocity*, Proc. Amer. Math. Soc. 47 (1975), pp. 333–334.

Received on 27.5.1983
and in revised form on 27.3.1984 (1362)