MATH. SCAND. 60 (1987), 52–62

RESOLUTION OF THE SIGN AMBIGUITY IN THE DETERMINATION OF THE CYCLOTOMIC NUMBERS OF ORDER 4 AND THE CORRESPONDING JACOBSTHAL SUM

S. A. KATRE and A. R. RAJWADE

1. Introduction.

In his Werke ([7, pp. 79–87]), Gauss, by a wholly elementary procedure, obtained formulae for cyclotomic numbers of order 4 for a prime $p \equiv 1 \pmod 4$, in terms of the quadratic partition $p = s_0^2 + t_0^2$, $s_0 \equiv 1 \pmod 4$, (which fixes s_0 uniquely and t_0 upto sign). This result may also be found in the work of Dickson ([5, pp. 400–401]). However, Gauss and Dickson did not resolve the sign ambiguity in t_0, viz. given a generator g of F_p^*, it is not clear which sign of t_0 gives correct formulae for the cyclotomic numbers corresponding to g. The corresponding result of M. Hall ([8, Theorem 3.2]) for F_q ($q = p^n \equiv 1 \pmod 4$) also has a similar sign ambiguity in the case when $p \equiv 1 \pmod 4$. (See also Storer [13, Lemmas 19, 19′, p. 48 and p. 51].) The main object of this paper is to resolve this sign ambiguity. Indeed we prove the following:

THEOREM 1. *Let p be an odd prime, $q = p^n \equiv 1 \pmod 4$, $q = 1 + 4f$. Let v be a generator of F_q^*. If $p \equiv -1 \pmod 4$, let $s = (-p)^{n/2}$ and $t = 0$. If $p \equiv 1 \pmod 4$, define s uniquely by $q = s^2 + t^2$, $p \nmid s$, $s \equiv 1 \pmod 4$, and then t uniquely by $v^{(q-1)/4} \equiv s/t \pmod p$. Then the cyclotomic numbers of order 4 for F_q, corresponding to v, are determined unambiguously by the following formulae:*

For f even,

$$
\begin{aligned}
A &= (0,0) = \tfrac{1}{16}(q - 11 - 6s), \\
B &= (0,1) = (1,0) = (3,3) = \tfrac{1}{16}(q - 3 + 2s + 4t), \\
C &= (0,2) = (2,0) = (2,2) = \tfrac{1}{16}(q - 3 + 2s), \\
D &= (0,3) = (3,0) = (1,1) = \tfrac{1}{16}(q - 3 + 2s - 4t), \\
E &= (1,2) = (2,1) = (1,3) = (3,1) = (2,3) = (3,2) = \tfrac{1}{16}(q + 1 - 2s),
\end{aligned}
$$

Received May 5, 1984; in revised form October 9, 1985.

and for f odd,

$$A = (0,0) = (2,0) = (2,2) = \tfrac{1}{16}(q-7+2s),$$
$$B = (0,1) = (1,3) = (3,2) = \tfrac{1}{16}(q+1+2s-4t),$$
$$C = (0,2) = \tfrac{1}{16}(q+1-6s),$$
$$D = (0,3) = (1,2) = (3,1) = \tfrac{1}{16}(q+1+2s+4t),$$
$$E = (1,0) = (1,1) = (2,1) = (2,3) = (3,0) = (3,3) = \tfrac{1}{16}(q-3-2s).$$

(This solves the cyclotomic problem in this case completely.)

Also, for $p \equiv 1 \pmod 4$, *if* s_0, t_0 *are uniquely determined by* $p = s_0^2 + t_0^2$, $s_0 \equiv 1 \pmod 4$, *and* $v^{(q-1)/4} \equiv s_0/t_0 \pmod p$, *then the s and t in the above formulae are given by*

$$s = s_0^n - \binom{n}{2} s_0^{n-2} t_0^2 + \binom{n}{4} s_0^{n-4} t_0^4 - \dots$$

and

$$t = t_0 \left[\binom{n}{1} s_0^{n-1} - \binom{n}{3} s_0^{n-3} t_0^2 + \dots \right].$$

The above described ambiguity for cyclotomic numbers of order 4 runs parallel to the sign ambiguity in the well known Jacobsthal sum defined by

$$\Phi_2(a) = \Phi_2(a; q) = \sum_{x \in F_q} \left(\frac{x(x^2+a)}{q} \right), \quad a \in F_q^*, \quad (q = p^n \equiv 1 \pmod 4),$$

where $(./q)$ is the Legendre symbol in F_q. This ambiguity is apparent in the following result of Jacobsthal ($q = p$ case) (see also [1, pp. 384–385]).

PROPOSITION (Jacobsthal [10], 1907). *For* $p \equiv 1 \pmod 4$, $p = s_0^2 + t_0^2$, $s_0 \equiv 1 \pmod 4$, *one has,*

$$\Phi_2(a; p) = \begin{cases} -2s_0, & \text{if } a \text{ is a fourth power } (\bmod p), \\ 2s_0, & \text{if } a \text{ is a square but not a fourth power } (\bmod p), \\ \pm 2t_0, & \text{if } a \text{ is not a square } (\bmod p). \end{cases}$$

The ambiguity in the sign of t_0 in the results of Jacobsthal remained unresolved for quite some time. In 1935, Davenport and Hasse ([4, § 7 II, pp. 176–178]) obtained $\Phi_2(a)$ in terms of the two normalized prime factors π, $\bar{\pi}$ of $p = \pi\bar{\pi}$ in $\mathbf{Z}[i]$ and the quartic residue symbol. (See the formulation of H. P. F. Swinnerton-Dyer in [3, p. 284] for the case $q = p$. From the formuls for N_p there, we get $\Phi_2(a; p)$ by $N_p = p + 1 + \Phi_2(-D; p)$.) The ambiguity in Jacobsthal's result was resolved by E. Lehmer ([12, Theorems 2 and 4]) in the case when 2 is a quartic nonresidue of $p \equiv 1 \pmod 4$.

Recently, Hudson and Williams [9], Evans [6], and Katre (independently) [11], have resolved this sign ambiguity completely in the case $q=p$ by different methods. However for $q=p^n$ $(n>1)$ only partial results are known. For $q=p^2$, see the results of Berndt and Evans (with sign ambiguities) in [2, Theorems 6.1 and 6.2]. For a general q, the result for $\Phi_2(1)$ may be found in Storer's book [13, p. 56]. The second aim of this paper is to obtain unambiguous results for $\Phi_2(a, p^n)$, $n \geqq 1$. This is achieved in the following

THEOREM 2. *Let $q=p^n \equiv 1 \pmod 4$. Let $a \in F_q$, $a \neq 0$. If $p \equiv -1 \pmod 4$, let $s=(-p)^{n/2}$ and $t=0$. If $p \equiv 1 \pmod 4$, define s uniquely by $q=s^2+t^2$, $p \nmid s$, $s \equiv 1 \pmod 4$, and in case a is not a square in F_q, define t uniquely in terms of a by $a^{(q-1)/4} \equiv s/t \pmod p$. Then $\Phi_2(a)$ is unambiguously given by*

$$\Phi_2(a) = \begin{cases} -2s & \text{if } a \text{ is a fourth power in } F_q, \\ 2s & \text{if } a \text{ is a square but not a fourth power in } F_q, \\ 2t & \text{if } a \text{ is not a square in } F_q. \end{cases}$$

Also, for $p \equiv 1 \pmod 4$, $q=p^n$, *if s_0 and t_0^2* are uniquely given by $p=s_0^2+t_0^2$, $s_0 \equiv 1 \pmod 4$, and in case a is not a square in F_q, t_0 is uniquely given by $a^{(q-1)/4} \equiv s_0/t_0 \pmod p$, then we have the alternative formulation

$$\Phi_2(a) = \begin{cases} -2\left[s_0^n - \binom{n}{2} s_0^{n-2} t_0^2 + \dots\right] & \text{if } a \text{ is a fourth power in } F_q, \\ 2\left[s_0^n - \binom{n}{2} s_0^{n-2} t_0^2 + \dots\right] & \text{if } a \text{ is a square but not a fourth power in } F_q, \\ 2t_0\left[\binom{n}{1} s_0^{n-1} - \binom{n}{3} s_0^{n-3} t_0^2 + \dots\right] & \text{if } a \text{ is not a square in } F_q. \end{cases}$$

In section 2, we give the proof of Theorem 1 and in section 3, that of Theorem 2. In section 4, we give an example.

REMARK. For $a, b \neq 0$ in F_q $(q \equiv 1 \pmod 4)$, Theorem 1 enables us to find the number N_1 of solutions of the equation $ax^4-by^4=1$ in F_q, this number being $16(k, h)+N_0(a)+N_0(-b)$, where for any chosen generator v of F_q^*, $h \equiv \operatorname{ind}_v a \pmod 4$, $k \equiv \operatorname{ind}_v b \pmod 4$, and for $u \in F_q^*$, $N_0(u)=4$ or 0 according as u is or is not a fourth power in F_q. Also, Theorem 2 enables us to find the number N_2 of solutions of $y^2=ax^4-b$, $a, b \in F_q^*$, since

$$N_2 = q+\sum_{x\in F_q}\left(\frac{ax^4-b}{q}\right) = q+(a/q)\sum\left(\frac{x^4-b/a}{q}\right)$$
$$= q+(a/q)\{\Phi_2(-b/a)-1\}\ .$$

The number of solutions of $y^2=x^3+ax$ in F_q is given by $q+\Phi_2(a)$.

2. The unique determination of cyclotomic numbers of order 4.

Let p be an odd prime, $q=p^n\equiv 1 \pmod 4$, $q=1+4f$, v be a generator of the cyclic group F_q^*, F_q being the finite field of q elements. Let χ be the character on F_q, satisfying $\chi(0)=0$, $\chi(v)=i$. Then for h,k modulo 4, the cyclotomic numbers (h,k) and the Jacobi sums $R(h,k)$ of order 4 are defined by

$$(h,k) = \text{the number of } v\in F_q \text{ such that } \operatorname{ind}_v v\equiv h \pmod 4 \text{ and } \operatorname{ind}_v(v+1)\equiv k \pmod 4\ ,$$
$$R(h,k) = \sum_{v\in F_q}\chi^h(v)\chi^k(1-v)\ .$$

(Here $\chi^0(0)=0$, unlike on p. 44 in [13].

Note that our $R(h,k)$ is the $J_\chi(h,k)$ defined on p. 44 of [13], and so by Lemma 15, p. 44 of [13], it is equal to the $R(h,k)$ defined on p. 43 therein, whenever none of h,k, $h+k$ is divisible by 4. By Lemma 13 of [13], we have $R(1,1)$, $\overline{R(1,1)}=q$ and by Lemma 14 of [13], $R(1,1)=(-1)^f R(2,1)$.

But

$$R(2,1)\sum_{v\neq 0,1}\chi^2(v)\chi(1-v)\ ,$$
$$= \sum_{v\neq 0,1}(\chi^2(v)+1)\chi(1-v)-\sum_{v\neq 0,1}\chi(1-v)\ ,$$
$$\equiv \sum_{v\neq 0,1}(\chi^2(v)+1)+\chi(1) \pmod{(2+2i)}\ ,$$
$$= -\chi^2(1)+q-2+1\ ,$$
$$= q-2 \equiv -1 \pmod{(2+2i)}\ .$$

This gives $R(1,1)\equiv(-1)^{f+1} \pmod{(2+2i)}$.

We note that if we write $R(1,1)=-s+it$, then $q=s^2+t^2$, and the congruence condition on $R(1,1)$ is equivalent to saying that $s\equiv 1 \pmod 4$.

LEMMA 1. *If $\alpha,\beta\in \mathbf{Z}[i]$ are comprime to $1+i$ and they satisfy $(\alpha)=(\beta)$, and $\alpha\equiv\beta \pmod{(2+2i)}$, then $\alpha=\beta$.*

PROOF. By the first condition, $\alpha=\beta\eta$, where η is a unit in $\mathbf{Z}[i]$, hence a root of unity. Since α,β are coprime to $1+i$, the second condition forces that $\eta\equiv 1 \pmod{(2+2i)}$. Hence $\eta=1$.

In view of this lemma, $R(1,1)$ is fixed completely if one knows the prime ideal decomposition of $R(1,1)$. We achieve this in what follows:

CASE (i). Let $p\equiv -1 \pmod 4$. Since $q\equiv 1 \pmod 4$, we get that n is even and so is f. p itself stays prime in $\mathbf{Z}[i]$ and so $R(1,1)\,\overline{R(1,1)}=q$ gives $(R(1,1))=(p)^{n/2}$ as ideals. This forces that $R(1,1)=-(-p)^{n/2}$. We have thus proved

PROPOSITION 1. *Let* $p\equiv -1 \pmod 4$, $q=p^n$, $q\equiv 1 \pmod 4$, *then the system of diophantine equations* $q=s^2+t^2$, $s\equiv 1 \pmod 4$ *has a unique solution* viz. $s=(-p)^{n/2}$, $t=0$. *For this solution,* $R(1,1)=-s+it$.

CASE (ii). Let $p\equiv 1 \pmod 4$. In this case p is the product of two distinct prime ideals in $\mathbf{Z}[i]$. Let $b=v^{(q-1)/4}$. Then $b\in \boldsymbol{F}_p$. By abuse of notation, let b also denote any rational integer $\equiv v^{(q-1)/4} \pmod p$. Then $(b-i)(b+i)\equiv 0 \pmod p$. One checks at once that there is a unique prime divisor $\mathfrak{p}$ of p which also divides $b-i$. Then $p=\mathfrak{p}\bar{\mathfrak{p}}$. We now have

LEMMA 2. *Let* $J=R(1,1)$. *Then* $\mathfrak{p}\mid J$ *but* $\mathfrak{p}\nmid \bar{J}$.

PROOF. For $k=1,3$, let σ_k be the automorphism of $\mathbf{Q}(i)$ satisfying $\sigma_k(i)=i^k$. Thus $J=J^{\sigma_1}$, $\bar{J}=J^{\sigma_3}$. Let

$$S_k = \sum_{v\in \boldsymbol{F}_q} v^{k(q-1)/4}(1-v)^{k(q-1)/4}.$$

Since $v^{(q-1)/4}\in \boldsymbol{F}_p$, S_k may be considered as an integer modulo p. We have,

$$\begin{aligned} J^{\sigma_k}-S_k &= \sum_{v\in \boldsymbol{F}_q}\left[\chi^k(v)\chi^k(1-v)-v^{k(q-1)/4}(1-v)^{k(q-1)/4}\right], \\ &= \sum_v \chi^k(v)\{\chi^k(1-v)-(1-v)^{k(q-1)/4}\}+ \\ &\quad +\sum_v (1-v)^{k(q-1)/4}\{\chi^k(v)-v^{k(q-1)/4}\}. \end{aligned}$$

Each term in the curly brackets is divisible by $b-i$ modulo p. Therefore, $J^{\sigma_k}\equiv 0 \pmod{\mathfrak{p}}$ if and only if $S_k\equiv 0 \pmod{\mathfrak{p}}$ if and only if $S_k\equiv 0 \pmod p$. Now

$$S_k = \sum_v v^{k(q-1)/4}(1-v)^{k(q-1)/4} = \sum_v \sum_{j=0}^{k(q-1)/4} (-1)^j v^{k(q-1)/4+j}\binom{k(q-1)/4}{j}.$$

But

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

This gives $S_1 \equiv 0 \pmod{p}$, and

$$S_3 \equiv (-1)^{(q-1)/4} \binom{3(q-1)/4}{(q-1)/4} \pmod{p}.$$

However for $x = 1, 2, 3$, the exact power of p dividing $(x(q-1)/4)!$ is $((q-1)/(p-1)-n)x/4$. Hence the exact power of p dividing $\binom{3(q-1)/4}{(q-1)/4}$ is $((q-1)/(p-1)-n) \cdot \frac{1}{4} \cdot (3-1-2) = 0$. Thus $S_3 \not\equiv 0 \pmod{p}$. This completes the proof of Lemma 2.

LEMMA 3. $(R(1,1)) = \mathfrak{p}^n$, *as ideals.*

PROOF. This follows from Lemma 2, noting that $(p) = \mathfrak{p}\bar{\mathfrak{p}}$ and $R(1,1)\overline{R(1,1)} = q = p^n$.

LEMMA 4. *For* $p \equiv 1 \pmod{4}$, *the conditions* $R(1,1) \equiv (-1)^{f+1} \pmod{(2+2i)}$, *and* $(R(1,1)) = \mathfrak{p}^n$, *fix* $R(1,1)$ *completely.*

PROOF. This follows from Lemma 1.

REMARK. For $p \equiv 1 \pmod{4}$, the number of solutions (s,t) of the equations $q = s^2 + t^2$, $s \equiv 1 \pmod{4}$ is equal to the number of ideals $\mathfrak{a}$ in $\mathbf{Z}[i]$ such that $\mathfrak{a}\bar{\mathfrak{a}} = q$. (More precisely, let (s_0, t_0) be any given solution of $p = s_0^2 + t_0^2$, $s_0 \equiv 1 \pmod{4}$. Then (s,t) is a solution of $q = s^2 + t^2$, $s \equiv 1 \pmod{4}$ if and only if $s + it = (s_0 + it_0)^j (s_0 - it_0)^{n-j}$ for some $0 \leqq j \leqq n$.) This number is $n+1$. We should like to know which of these $n+1$ solutions gives rise to $R(1,1) = -s + it$. For this we first note that of these $n+1$ solutions there are exactly two solutions such that $p \nmid (-s+it)$, viz. those for which $-s+it$ has prime ideal factorization $\mathfrak{p}^n$ or $\bar{\mathfrak{p}}^n$. Hence these two solutions correspond to $R(1,1)$ and $\overline{R(1,1)}$. Also, $p \nmid (-s+it)$ is equivalent to saying that $p \nmid s$. (This follows from $q = s^2 + t^2$.) We have thus proved

PROPOSITION 2. *For* $p \equiv 1 \pmod{4}$, *if* s *and* t *satisfy* $q = s^2 + t^2$, $p \nmid s$, $s \equiv 1 \pmod{4}$, *then* $-s + it = R(1,1)$ or $\overline{R(1,1)}$ *and conversely.*

Compare with Theorem 3.2 in [7] and Lemma 18 of [10]).

The proposition shows that the diophantine conditions $q = s^2 + t^2$, $p \nmid s$, $s \equiv 1 \pmod{4}$ determine s uniquely and t upto sign. We now determine which t gives $R(1,1) = -s + it$ with the aid of the following

LEMMA 5. *For* $p \equiv 1 \pmod 4$, *let* $q = s^2 + t^2$, $p \nmid s$. *Then* $\mathfrak{p} \mid (-s+it)$ *if and only if* $b \equiv s/t \pmod p$.

PROOF. The conditions $q = s^2 + t^2$, $p \nmid s$ imply that $-s+it$ is the power of a single prime divisor of p. Hence $\mathfrak{p} \mid (-s+it)$ if and only if $p \mid (b-i)(-s-it)$, and noting that $b \equiv i \pmod{\mathfrak{p}}$ if and only if $-s+it \equiv t(b-s/t) \pmod{\mathfrak{p}}$, the lemma follows.

COROLLARY. *For* $p = s_0^2 + t_0^2$, $\mathfrak{p} = (-s_0 + it_0)$ *if and only if* $b \equiv s_0/t_0 \pmod p$.

Since $\mathfrak{p} \mid R(1,1)$ but not $\overline{R(1,1)}$ we have

PROPOSITION 3. *Let* $p \equiv 1 \pmod 4$. *Let* $s, t \in \mathbf{Z}$ *be uniquely determined by* $q = s^2 + t^2$, $p \nmid s$, $s \equiv 1 \pmod 4$, *and* $v^{(q-1)/4} \equiv s/t \pmod p$. *Then* $R(1,1) = -s + it$ *and conversely.*

LEMMA 6. *Let* $p \equiv 1 \pmod 4$. *Then with obvious notation* $R(1,1;q) = (-1)^{n+1}(R(1,1;p))^n$, *where* $R(1,1;p)$ *corresponds to a primitive root* $g \bmod p$ *satisfying* $g^{(p-1)/4} \equiv v^{(q-1)/4} \pmod p$.

PROOF. Each side has absolute value $\sqrt{q}$, and each side has prime ideal factorization $\mathfrak{p}^n$ where $\mathfrak{p}$ is the unique prime divisor of p which also divides $v^{(q-1)/4} - i = g^{(q-1)/4} - i$. Also, if $q = 1 + 4f$ and $p = 1 + 4f_0$, then $(-1)^f = (-1)^{nf_0}$, so each side has the same residue $(-1)^{f+1} \pmod{(2+2i)}$. Hence the result follows by Lemma 1.

PROPOSITION 4. *Let* $p \equiv 1 \pmod 4$. *Let* s *and* t *be as in Proposition* 3 *and let* s_0, t_0 *be uniquely determined by* $p = s_0^2 + t_0^2$, $s_0 \equiv 1 \pmod 4$, *and* $v^{(q-1)/4} \equiv s_0/t_0 \pmod p$. *Then*

$$s = s_0^n - \binom{n}{2} s_0^{n-2} t_0^2 + \binom{n}{4} s_0^{n-4} t_0^4 - \dots,$$

and

$$t = t_0 \left[\binom{n}{1} s_0^{n-1} - \binom{n}{3} s_0^{n-3} t_0^2 + \dots \right].$$

PROOF. Under the given conditions, $R(1,1;p) = -s_0 + it_0$ (g to be chosen as in Lemma 6). Hence by Lemma 6,

$$-s+it = (-1)^{n+1}(-s_0+it_0)^n = -(s_0-it_0)^n.$$

Thus

$$s-it = (s_0-it_0)^n$$

$$= \left[s_0^n - \binom{n}{2}s_0^{n-2}t_0^2 + \binom{n}{4}s_0^{n-4}t_0^4 - \dots\right] -$$

$$-it_0\left[\binom{n}{1}s_0^{n-1} - \binom{n}{3}s_0^{n-3}t_0^2 + \binom{n}{5}s_0^{n-5}t_0^4 - \dots\right].$$

REMARK. In view of Proposition 4, for $p \equiv 1 \pmod 4$ one now does not require to find the values of s and t in $q = s^2+t^2$, $p \nmid s$, $s \equiv 1 \pmod 4$, by trial for each n separately; it is sufficient to know the result just for $n=1$. Trials to find both s and s_0 may also be avoided using the results of Gauss (for s_0) and Storer (for s) (see Theorem 8, p. 52 of [13]) viz. $2s_0$ is the unique even integer between $-p$ and p which is congruent to $\binom{2f_0}{f_0} \pmod p$, where $p = 1+4f_0$, and $2s$ is the unique even integer between $-q$ and q which is congruent to $\binom{2f}{f} \pmod q$, where $q = p^n = 1+4f$.

LEMMA 7. *Let* $q \equiv 1 \pmod 4$. (p *may be* $\equiv \pm 1 \pmod 4$.) *For a given generator* v *of* $\mathbf{F}_q^*$, *write* $R(1,1) = -s+it$. *Then the cyclotomic numbers of order* 4 *for* $\mathbf{F}_q$, *related to* v, *are those given in the statement of Theorem* 1.

PROOF. This result follows from the calculations in the proofs of Lemmas 19 and 19′ on pp. 48–51 of [13]. For $q=p$, the formulae appear in the work of Gauss ([7, p. 83 and 87]) or Dickson ([5, pp. 400–401]).

PROOF OF THEOREM 1. This now follows by combining Propositions 1, 3, 4 with Lemma 7.

3. The evaluation of the Jacobsthal sum $\Phi_2(a)$ in $\mathbf{F}_q$.

The Jacobsthal sum $\Phi_2(a)$, for $\mathbf{F}_q$, $q \equiv 1 \pmod 4$, $a \in \mathbf{F}_q$, $a \neq 0$, is defined by

$$\Phi_2(a) = \sum_{v \in \mathbf{F}_q} \left(\frac{v(v^2+a)}{q}\right),$$

where $(\cdot/q)$ is the Legendre symbol in $\mathbf{F}_q$. (The Jacobsthal sum may be defined even if $a=0$ or $q \not\equiv 1 \pmod 4$, but then it is trivial to evaluate it.) The theory developted in section 2 will enable us to evaluate $\Phi_2(a)$ correctly and thus remove the sign ambiguity of Jacobsthal and later authors. To this end we first have

LEMMA 8. $\Phi_2(a) = (a/q)[\chi(a)R(1,1) + \overline{\chi(a)R(1,1)}]$.

PROOF. By Theorem 2.7, p. 376 of [2],

$$\begin{aligned}\Phi_2(a) &= \chi(-1)[\chi^{2+1}(a)\chi(4)R(1,1)+\chi^{2+3}(a)\chi(4)R(3,3)] \\ &= \chi(-4)\chi^2(a)[\chi(a)R(1,1)+\overline{\chi(a)R(1,1)}] .\end{aligned}$$

But for $q\equiv 1 \pmod 4$, -4 is a fourth power in F_q. Also $\chi^2(a)=(a/q)$. This proves the lemma.

PROOF OF THEOREM 2. For $q\equiv 1 \pmod 4$, let $R(1,1;\, q)=-s+it$, and in case $p\equiv 1 \pmod 4$, let $R(1,1;\, p)=-s_0+it_0$, where g and v are related as in Lemma 6. Then

$$s = s_0^n-\binom{n}{2}s_0^{n-2}t_0^2+\ldots, \quad \text{and}$$

$$t = t_0\left[\binom{n}{1}s_0^{n-1}-\binom{n}{3}s_0^{n-3}t_0^2+\ldots\right].$$

If $p\equiv -1 \pmod 4$, $s=(-p)^{n/2}$, $t=0$. If $p\equiv 1 \pmod 4$, s, s_0 are determined uniquely by $q=s^2+t^2$, $p\nmid s$, $s\equiv 1 \pmod 4$, and $p=s_0^2+t_0^2$, $s_0\equiv 1 \pmod 4$ respectively. If a is a fourth power in F_q, then

$$\begin{aligned}\Phi_2(a) &= -s+it+(-s-it) \\ &= -2s .\end{aligned}$$

If a is a square but not a fourth power in F_q, then

$$\begin{aligned}\Phi_2(a) &= s-it+(s+it) \\ &= 2s .\end{aligned}$$

Let now a be a nonsquare in F_q. Let v be a chosen generator of F_q^* satisfying

$$v^{(q-1)/4} \equiv a^{(q-1)/4} \pmod p .$$

Then t, t_0 are uniquely determined by

$$a^{(q-1)/4} \equiv \frac{s}{t} = \frac{s_0}{t_0} \pmod p .$$

Also it follows that for the chosen v, $\chi(a)=i$.

Thus

$$\begin{aligned}\Phi_2(a) &= -[i(-s+it)-i(-s-it) \\ &= 2t .\end{aligned}$$

This proves the theorem.

4. An example.

Let $p=5$, $q=p^2=25=1+4f$. Thus f is even, $q=s^2+t^2$, $s\equiv 1 \pmod 4$ has three solutions viz. $(-3, \pm 4)$ and $(5,0)$. The condition $p \nmid s$ rejects the last solution. Thus $s=-3$, $t=\pm 4$. Take

$$F_q = \{l+m\omega \mid l,m \pmod 5,\ \omega^3=1,\ \omega \neq 1\}.$$

For the generator $v=2+\omega$ of F_q^*,

$$v^{(q-1)/4} = v^6 \equiv -2 \pmod 5.$$

Hence the condition $v^{(q-1)/4} \equiv s/t \pmod p$ gives $t=4$. Thus using the formulae in Theorem 1 for f even, the cyclotomic numbers (i,j) of order 4 in F_q corresponding to v are correctly given by the matrix

i \ j	0	1	2	3
0	2	2	1	0
1	2	0	2	2
2	1	2	1	2
3	0	2	2	2

which may be verified by direct calculation also.

For $a=-2+\omega$, $a^{(q-1)/4} \equiv s/t \pmod p$ gives $t=-4$, so $\Phi_2(a)=2t=-8$ by Theorem 2. This agrees with the result obtained by direct calculation, since it may be checked that for $x \neq 0$, x^3+ax is a square for 8 values of x and a nonsquare for 16 values of x, so that $\Phi_2(a)=8-16=-8$.

Note that the s_0, t_0 of Theorems 1 and 2 in these cases are respectively $1,2$ and $1,-2$, and they yield correct results.

REFERENCES

1. B. C. Berndt and R. J. Evans, *Sums of Gauss, Jacobi, and Jacobsthal*, J. Number Theory 11 (1979), 349–398.
2. B. C. Berndt and R. J. Evans, *Sums of Gauss, Eisenstein, Jacobi, Jacobsthal, and Brewer*, Illinois J. Math. 23 (1979), 374–437.
3. J. W. S. Cassels and A. Fröhlich, *Algebraic number theory*, (Proc. Conf. Brighton, 1965), p. 284. Academic Press, London, New York, 1967.
4. H. Davenport and H. Hasse, *Die Nullstellen der Kongruenzzetafunktionen in gewissen zyklischen Fallen*, J. Reine Angew. Math. 172 (1935), 151–182.
5. L. E. Dickson, *Cyclotomy, higher congruences, and Waring's problem*, Amer. J. Math. 57 (1935), 391–424.
6. R. J. Evans, *Determination of Jacobsthal sums*, Pacific J. Math., to appear.
7. C. F. Gauss, *Theoria Residuorum Biquadraticorum*, Werke, vol. 2 (1876), 67–92.
8. M. Hall, Jr., *Characters and cyclotomy*, (Proc. Symp. Pure Math. 8), pp. 31–43. Amer. Math. Soc., Providence, R.I., 1965.

9. R. H. Hudson and K. S. Williams, *Resolution of ambiguities in the evaluation of cubic and quartic Jacobsthal sums*, Pacific J. Math. 99 (1982), 379–386.
10. E. Jacobsthal, *Über die Darstellung der Primzahlen der Form* $4n+1$ *als Summe zweier quadrate*, J. Reine Angew. Math. 132 (1907), 238–245.
11. S. A. Katre, *Jacobsthal sums in terms of quadratic partitions of a prime*, (Proc. conference in Number Theory held at Ootacamund, India, 1984). To appear in Lecture Notes series Springer-Verlag.
12. E. Lehmer, *On the number of solutions of* $u^k + D \equiv w^2 \pmod{p}$, Pacific J. Math. 5 (1955), 103–118.
13. T. Storer, *Cyclotomy and difference sets* I, Markham Publ. Co., Chicago, 1967.

CENTRE FOR ADVANCED STUDY IN MATHEMATICS
PANJAB UNIVERSITY
CHANDIGARH, 160014
INDIA