

THEOREMS ON BREWER SUMS

S. F. ROBINSON

Let $V_m(x, Q)$ be the polynomial determined by the recurrence relation

$$(1.1) \quad V_{m+2}(x, Q) = x \cdot V_{m+1}(x, Q) - Q \cdot V_m(x, Q)$$

($m = 1, 2, \dots$), Q an integer, with $V_1(x, Q) = x$ and $V_2(x, Q) = x^2 - 2Q$. In a recent paper, B. W. Brewer has defined the sum

$$(1.2) \quad A_m(Q) = \sum_{x=0}^{p-1} \chi(V_m(x, Q))$$

where $\chi(s)$ denotes the Legendre symbol (s/p) with p and odd prime.

The purpose of this paper is to consider the evaluation of $A_{2n}(Q)$ when n is odd. The principle result obtained is the expression of $A_{2n}(Q)$ as the sum of $\chi(Q) \cdot A_n(1)$ and one half the character sum $\phi_{2e}(1)$. $\phi_{2e}(1)$ can in turn be expressed in terms of the Gaussian cyclotomic numbers (i, j) . The values of $A_6(Q)$ and $A_{10}(Q)$ follow immediately from this result utilizing values for $A_3(1) = A_3$ and $A_5(1) = A_5$ computed by B. W. Brewer and A. L. Whiteman.

2. The character sums $\Omega_m(Q)$ and $\theta_m(Q)$ and Brewer's lemma. Let p be an odd prime and λ a generating element of the multiplicative group of $GF(p^2)$. Then $\lambda^{p+1} = g$ is a primitive root of $GF(p)$. Set $Q = g^r = \lambda^{r(p+1)}$, $0 \leq r < p-1$. In order to facilitate the evaluation of $A_m(Q)$, Brewer defines the following two sums:

$$(2.1) \quad \begin{aligned} \Omega_m(Q) &= \sum_{s=1}^{p-1} \chi(\lambda^{ms(p+1)} + Q^m \lambda^{ms(p+1)}) \\ &= \sum_{s=1}^{p-1} \chi(g^{ms} + g^{mr} g^{-ms}) \end{aligned}$$

and

$$(2.2) \quad \begin{aligned} \theta_m(Q) &= \sum_{t=1}^{p+1} \chi(\lambda^{m(t(p-1)+r)} + Q^m \lambda^{-m(t(p-1)+r)}) \\ &= \sum_{t=1}^{p+1} \chi(\lambda^{m(t(p-1)+r)} + \lambda^{mr(p+1)} \lambda^{-m(t(p-1)+r)}) . \end{aligned}$$

Brewer relates the sums $\Omega_m(Q)$ and $\theta_m(Q)$ to the sum $A_m(Q)$ by the equation [2, Lemma 2].

$$(2.3) \quad 2A_m(Q) = \theta_m(Q) + \Omega_m(Q) .$$

(Compare also [1, Lemma 2] and [14, Lemma 1].)

The following theorem is fundamental [2, Th. 1].

THEOREM 2.1. *Let p be an odd prime, $A_m(Q)$ be defined as in (1.2). If $\chi(Q') = \chi(Q)$ and $Q' \equiv n^2Q \pmod{p}$, then $A_m(Q') = \chi(n)^m A_m(Q)$, ($m = 1, 2, \dots$).*

3. The Jacobsthal sum. Closely related to the Brewer sum are the character sums of Jacobsthal

$$(3.1) \quad \phi_e(n) = \sum_{h=1}^{p-1} \chi(h) \chi(h^e + n)$$

and the related sum

$$(3.2) \quad \psi_e(n) = \sum_{h=1}^{p-1} \chi(h^e + n) .$$

We note

$$A_2(Q) = \sum_{x=0}^{p-1} \chi(x^2 - 2Q) = \psi_2(-2Q) + \chi(-2Q)$$

and

$$A_3(Q) = \sum_{x=0}^{p-1} \chi(x^3 - 3Qx) = \phi_3(-3Q) .$$

In general if m is even and g a primitive root of p

$$(3.3) \quad \begin{aligned} \Omega_m(Q) &= \sum_{s=1}^{p-1} \chi(g^{ms} + Q^m g^{-ms}) \\ &= \psi_{2m}(Q^m) , \end{aligned}$$

while if m is odd

$$(3.4) \quad \begin{aligned} \Omega_m(Q) &= \sum_{s=1}^{p-1} \chi(g^{ms} + Q^m g^{-ms}) \\ &= \sum_{s=1}^{p-1} \chi(g^{-ms}) \cdot \chi(g^{2ms} + Q^m) \\ &= \sum_{s=1}^{p-1} \chi(g^{-(m+1)s}) \cdot \chi(g^s) \cdot \chi(g^{2ms} + Q^m) \\ &= \phi_{2m}(Q^m) . \end{aligned}$$

The following results concerning Jacobsthal sums will be applied: if $p \nmid x$ [10, Equation 3.8]

$$(3.5) \quad \psi(nx^e) = \chi(x)^e \cdot \psi_e(n) ,$$

the reduction formula [10, Equation 3.9] and [7, Equation 6]

$$(3.6) \quad \phi_e(n) + \psi_e(n) = \psi_{2e}(n)$$

and [7, Formula 10] if e is odd

$$(3.7) \quad \psi_{2e}(n) = \phi_e(n) + \chi(n) \cdot \phi_e(n')$$

where $n \cdot n' \equiv 1 \pmod{p}$.

4. **Cyclotomy.** Let p be an odd prime and g a primitive root of p . Let e be a divisor of $p-1$, $p-1 = e \cdot f$. The cyclotomic number of order e , (i, j) is the number of solutions of $1 + g^{es+i} \equiv g^{et+j} \pmod{p}$, $s, t = 0, 1, \dots, f-1$.

If we write $2ef = p-1$,

$$\begin{aligned} \psi_{2e}(1) &= \sum_{s=0}^{p-1} \chi(g^{2es} + 1) \\ &= 2e \sum_{s=0}^{f-1} \chi(g^{2es} + 1) \\ \chi(g^{2es} + 1) &= \begin{cases} 1 & g^{2es} + 1 \equiv g^{2et+a} \pmod{p} \text{ } a \text{ even} \\ -1 & g^{2es} + 1 \equiv g^{2et+a} \pmod{p} \text{ } a \text{ odd} . \end{cases} \end{aligned}$$

Thus in this case $\psi_{2e}(1)$ can be expressed in terms of the cyclotomic numbers of order $2e$

$$(4.1) \quad \psi_{2e}(1) = \frac{1}{2e} \sum_{i=0}^{2e-1} (-1)^i (2e)^2(0, i) .$$

In the theory of cyclotomy, the Jacobi sum and the related Lefrange resolvent play a fundamental role. In what follows we will use some of the properties of the Jacobi sum.

Let $\beta = \exp(2\pi i/e)$, $e \cdot f + 1 = p$. The Jacobi sum is defined by the equation

$$(4.2) \quad \psi(\beta^m, \beta^n) = \sum_{\substack{a+b=1 \pmod{p} \\ 1 \leq a, b \leq p-1}} \beta^{m \text{ ind } a + n \text{ ind } b}$$

The following equalities for the Jacobi sum can be derived: [12, Formula 2.4]

$$(4.3) \quad \psi(\beta^m, \beta^n) = \psi(\beta^n, \beta^m) = (-1)^{nf} \psi(\beta^{-m-n}, \beta^n) .$$

Placing $n = 0$ in (4.2) we have [12, Formula 2.5]

$$(4.4) \quad \psi(\beta^m, \beta^0) = \begin{cases} p-2 & m=0 \\ -1 & 1 \leq m \leq e-1 \end{cases}$$

and the important formula

$$(4.5) \quad \psi(\beta^m, \beta^n) \cdot \psi(\beta^{-m}, \beta^{-n}) = p$$

provided e does not divide m, n or $m+n$.

Since $\psi(\beta^m, \beta^n)$ is periodic in both m and n with respect to e , it may be expanded into a double finite fourier series [11, Formula 2.6]

$$(4.6) \quad \psi(\beta^m, \beta^n) = (-1)^{mf} \sum_{h, k=0}^{e-1} (h, k) \beta^{mh+nk}.$$

We may also write (4.6) in the inverted form [11, Formula 2.7]

$$(4.7) \quad e^2(h, k) = \sum_{m, n=0}^{e-1} (-1)^{mf} \psi(\beta^m, \beta^n) \beta^{-mh-nk}.$$

In (4.6) replace m by vn , where v is an integer, collecting the exponents of β in the same residue class modulo e , we get an alternate form of the finite fourier series expansion [11, Equation 2.8]

$$(4.8) \quad \psi(\beta^{vn}, \beta^n) = (-1)^{vnf} \sum_{i=0}^{e-1} B(i, v) \beta^{ni}$$

where the fourier coefficients $B(i, v)$ are the Dickson-Hurwitz sums

$$(4.9) \quad B(i, v) = \sum_{h=0}^{e-1} (h, i - vh).$$

The inverted form of (4.8) is

$$(4.10) \quad e \cdot B(i, v) = \sum_{n=0}^{e-1} (-1)^{vnf} \psi(\beta^{vn}, \beta^n) \beta^{-ni}.$$

If $e \cdot f = p - 1$, Whiteman [10, Formula 5.8] expresses the Jacobsthal sum in terms of the cyclotomic function $B(i, v)$

$$(4.11) \quad eB(v, 1) = \begin{cases} p - 1 + \phi_e(4g^v) & e \text{ odd} \\ p - 1 + \psi_e(4g^v) & e \text{ even.} \end{cases}$$

Thus if $e \cdot f = p - 1$ with e odd, from (3.7) and (4.11) we can write

$$(4.12) \quad \begin{aligned} \psi_{2e}(1) &= 2\phi_e(1) \\ &= 2(e \cdot B(i, 1) - (p - 1)) \\ &= 2e(B(i, 1) - f) \end{aligned}$$

where i is selected so that $4g^i \equiv 1 \pmod{p}$.

5. The evaluation of $A_{2n}(Q)$ for odd values of n . In this section we will develop our principle result in the evaluation of $A_{2n}(Q)$ for odd values of n . We will consider $\Omega_{2n}(Q)$ and $\theta_{2n}(Q)$ separately and combine the results by use of equation (2.3).

THEOREM 5.1. *If d is the g.c.d. of m and $p + 1$ and $Q = \lambda^{r(p+1)}$ then*

$$(5.1) \quad \phi(Q) = \theta_d(Q^{m/d}).$$

Proof. This theorem is a direct result of the fact that if the

g.c.d. of a and M is d , and $\{r_1, r_2, \dots, r_M\}$ is a complete residue system modulo M , then the set $\{a \cdot r_1, a \cdot r_2, \dots, a \cdot r_M\}$ contains the same elements modulo M as the set $\{d \cdot r_1, d \cdot r_2, \dots, d \cdot r_M\}$. Now if the g.c.d. of m and $p+1$ is d , then

$$\begin{aligned}\theta_m(Q) &= \sum_{i=1}^{p+1} \chi(\lambda^{m(i(p-1)+r)} + \lambda^{mr(p+1)} \lambda^{-m(i(p-1)+r)}) \\ &= \sum_{i=1}^{p+1} \chi(\lambda^{d(i(p-1)+(mr/d))} + \lambda^{d(m/d)r(p+1)} \lambda^{-d(i(p-1)+(mr/d))}) \\ &= \theta_d(Q^{m/d}).\end{aligned}$$

We note $d < m$ unless $p \equiv -1 \pmod{m}$. This exceptional case is considered in the following two theorems.

THEOREM 5.2. *If $p = (4m) \cdot f - 1$*

$$(5.2) \quad \theta_m(Q) = \theta_{2m}(Q) = 0.$$

Proof. $\{2m \cdot 1, 2m \cdot 2, \dots, 2m \cdot (p+1)/2m\}$ has the same elements as $\{2m \cdot 1 + 2mf, 2m \cdot 2 + 2mf, \dots, 2m \cdot (p+1)/2m + 2mf\}$ modulo $p+1$. Also $\{m \cdot 1, m \cdot 2, \dots, m \cdot (p+1)/m\}$ has the same elements modulo $p+1$ as $\{m \cdot 1 + 2mf, m \cdot 2 + 2mf, \dots, m \cdot (p+1)/m + 2mf\}$. Since $\chi(\lambda^{2mf(p-1)}) = \chi(\lambda^{(p^2-1)/2}) = -1$ when $p \equiv 3 \pmod{4}$, we have

$$\begin{aligned}\theta_{2m}(Q) &= 2m \sum_{i=1}^{(p+1)/2m} \chi(\lambda^{2m(i(p-1)+r)} + Q^{2m} \lambda^{-2m(i(p-1)+r)}) \\ &= 2m \sum_{i=1}^{(p+1)/2m} \chi(\lambda^{2m(i(p-1)+r)+(p^2-1)/2} + Q^{2m} \lambda^{-2m(i(p-1)+r)+(p^2-1)/2}) \\ &= 2m \chi\left(\lambda^{\frac{p^2-1}{2}}\right) \sum_{i=1}^{(p+1)/2m} \chi(\lambda^{2m(i(p-1)+r)} + Q^{2m} \lambda^{-2m(i(p-1)+r)}) \\ &= -\theta_{2m}(Q)\end{aligned}$$

and

$$\begin{aligned}\theta_m(Q) &= m \sum_{i=1}^{(p+1)/m} \chi(\lambda^{m(i(p-1)+r)} + Q^m \lambda^{-m(i(p-1)+r)}) \\ &= m \sum_{i=1}^{(p+1)/m} \chi(\lambda^{m(i(p-1)+r)+(p^2-1)/2} + Q^m \lambda^{-m(i(p-1)+r)+(p^2-1)/2}) \\ &= -\theta_m(Q).\end{aligned}$$

THEOREM 5.3. *If $p = (2f+1)m - 1$ with $m \equiv 2 \pmod{4}$ and $Q = \lambda^{r(p+1)}$, then*

$$(5.3) \quad \theta_m(Q) = \theta_{m/2}(Q^2).$$

Proof. Since now $p \equiv 1 \pmod{4}$, $\chi(\lambda^{p^2-1/2}) = 1$. Let $F = 2f+1$. The set $\{m \cdot 1, m \cdot 2, \dots, m \cdot (p+1)/m\} \cup \{m \cdot 1 + (m \cdot F/2), m \cdot 2 + m \cdot F/2,$

$\dots, m \cdot p + 1/m + mF/2\}$ has the same elements as the set $\{m/2 \cdot 1, m/2 \cdot 2, \dots, m/2 \cdot 2(p+1)/m\}$ modulo $p+1$. Thus

$$\begin{aligned}\theta_m &= m \sum_{i=1}^{(p+1)/m} \chi(\lambda^{m(i(p-1)+r)} + \lambda^{mr(p+1)} \lambda^{-m(i(p-1)+r)}) \\ &= \frac{m}{2} \sum_{i=1}^{(p+1)/m} \chi(\lambda^{m(i(p-1)+r)} + \lambda^{mr(p+1)} \lambda^{-m(i(p-1)+r)}) \\ &\quad + \frac{m}{2} \chi(\lambda^{p^2-1/2}) \sum_{i=1}^{(p+1)/m} \chi(\lambda^{m(i(p-1)+r)} + \lambda^{mr(p+1)} \lambda^{-m(i(p-1)+r)}) \\ &= \frac{m}{2} \sum_{i=1}^{(2(p+1)/m)} \chi(\lambda^{m/2(i(p-1)+2r)} + \lambda^{m/22r(p+1)} \lambda^{-(m/2)(i(p-1)+r)}) \\ &= \theta_{m/2}(Q^2) .\end{aligned}$$

THEOREM 5.4. *If n is odd and p is an odd prime, then*

$$(5.4) \quad \theta_{2n}(Q) = \theta_n(Q^2) .$$

Proof. If $p \equiv -1 \pmod{n}$, the result follows from Theorems 5.2 and 5.3. If $p \not\equiv -1 \pmod{n}$, let the g.c.d. of n and $p+1$ be d . Then the g.c.d. of $2n$ and $p+1$ is $2d$ and $p \equiv -1 \pmod{d}$. Thus $\theta_{2n}(Q) = \theta_{2d}(Q^{n/d}) = \theta_d(Q^{2n/d}) = \theta_n(Q^2)$.

THEOREM 5.5. *If n is odd and the g.c.d. of $p-1$ and n is e , then*

$$(5.5) \quad \Omega_{2n}(Q) = \psi_{2e}(1) + \Omega_n(Q^2) .$$

Proof. From equations (3.3), (3.4), and (3.6) we can write

$$(5.6) \quad \begin{aligned}\Omega_{2n}(Q) &= \psi_{4n}(Q^{2n}) = \psi_{2n}(Q^{2n}) + \phi_{2n}(Q^{2n}) \\ &= \psi_{2n}(Q^{2n}) + \Omega_n(Q^2) .\end{aligned}$$

By equation (3.5) $\psi_{2n}(Q^{2n}) = \chi(Q)^{2n} \cdot \psi_{2n}(1) = \psi_{2n}(1)$. Now applying the reasoning used in Theorem 5.1 with g a primitive root of p

$$(5.7) \quad \begin{aligned}\psi_{2n}(1) &= \sum_{h=1}^{p-1} \chi(h^{2n} + 1) \\ &= \sum_{r=1}^{p-1} \chi(g^{2nr} + 1) \\ &= \sum_{r=1}^{p-1} \chi(g^{2er} + 1) \\ &= \psi_{2e}(1) .\end{aligned}$$

The result now follows from (5.6) and (5.7).

We can now state the basic tool for the evaluation of $\mathcal{A}_{2n}(Q)$ when n is odd.

Combining the results of Theorem 5.4 and 5.5 along with Equation 2.3, we have

THEOREM 5.6. *Assume n is odd. Let e be the g.c.d. of n and $p - 1$, then*

$$(5.8) \quad A_{2n}(Q) = A_n(Q^2) + \frac{1}{2}\psi_{2e}(1) .$$

Applying Theorem 2.1 we can write

$$(5.9) \quad A_{2n}(Q) = \chi(Q) \cdot A_n(1) + \frac{1}{2}\psi_{2e}(1) .$$

COROLLARY. *If n is an odd prime, $p \nmid Q$ and $p \not\equiv 1 \pmod{n}$*

$$(5.10) \quad A_{2n}(Q) = \chi(Q) \cdot A_n(1) - 1 .$$

6. The evaluation of $A_6(Q)$. The values of $A_6(Q)$ depend upon the decompositions $p = x^2 + 4y^2$ and $p = A^2 + 3B^2$ with the signs selected so that $x \equiv 1 \pmod{4}$, $2y \equiv x \pmod{3}$ and $A \equiv 1 \pmod{3}$.

$p \not\equiv 1 \pmod{6}$. By the corollary to Theorem 5.6,

$$A_6(Q) = \chi(Q) \cdot A_3(1) - 1 .$$

Brewer [1] and Whiteman [14] have evaluated $A_3(1) = A_3$ with the results

$$(6.1) \quad A_3(1) = \begin{cases} 0 & p \equiv 3 \pmod{4} \\ 4y & p \equiv 5 \pmod{12} \\ 2x & p \equiv 1 \pmod{12} \quad 3 \mid x \\ -2x & p \equiv 1 \pmod{12} \quad 3 \nmid x . \end{cases}$$

Thus we have for $A_6(Q)$ when $p \not\equiv 1 \pmod{6}$.

$$(6.2) \quad A_6(Q) = \begin{cases} \chi(Q) \cdot 4y - 1 & p \equiv 5 \pmod{12} \\ -1 & p \equiv 11 \pmod{12} \end{cases}$$

$p \equiv 1 \pmod{6}$. By Equation (5.9)

$$(6.3) \quad A_6(Q) = \chi(Q) \cdot A_3 + \frac{1}{2}\psi_6(1) .$$

In this case (4.1) becomes

$$(6.4) \quad \psi_6(1) = \frac{1}{6} \sum_{i=0}^5 \{36(0, 2i) - 36(0, 2i + 1)\} .$$

The values for the $36(o, h)$ can be determined from tables such as those given by Hall [4, p. 981] or computed directly using Equation (4.7) which becomes

$$(6.5) \quad 36(o, k) = \sum_{m, n=0}^5 (-1)^{mf} \psi(\beta^m, \beta^n) \beta^{-nk}$$

where $\beta = \exp(2\pi i)/6$. We can write

$$(6.6) \quad \psi_6(1) = \frac{1}{6} \sum_{m, n=0}^5 (-1)^{mf} \psi(\beta^m, \beta^n) \sum_{j=0}^5 (-1)^j \beta^{-nj}.$$

The right side of (6.6) reduces to

$$(6.7) \quad \begin{aligned} & \frac{1}{6} \sum_{m=0}^5 (-1)^{mf} \psi(\beta^m, \beta^3) \sum_{j=0}^5 (-1)^j \beta^{-3j} \\ &= \psi(\beta^0, \beta^3) + (-1)^f \psi(\beta^1, \beta^3) \\ & \quad + \psi(\beta^2, \beta^3) + (-1)^f \psi(\beta^3, \beta^3) + \psi(\beta^4, \beta^3) + (-1)^f \psi(\beta^5, \beta^3). \end{aligned}$$

By (4.3) and (4.4) we have

$$(6.8) \quad \begin{aligned} (-1)^f \psi(\beta^3, \beta^3) &= \psi(\beta^0, \beta^3) = -1 \\ \psi(\beta^1, \beta^3) &= (-1)^f \psi(\beta^2, \beta^1) \\ \psi(\beta^2, \beta^3) &= \psi(\beta^2, \beta^1) \\ \psi(\beta^4, \beta^3) &= \psi(\beta^5, \beta^4) \\ \psi(\beta^5, \beta^3) &= (-1)^f \psi(\beta^5, \beta^4). \end{aligned}$$

Set

$$\psi(\beta^2, \beta^1) = -A + B\sqrt{-3}$$

Then $\psi(\beta^5, \beta^4) = -A - B\sqrt{-3}$.

Dickson [2, p. 410] proved if $\psi(\beta^2, \beta^1) = -A + B\sqrt{-3}$, then $A \equiv 1 \pmod{3}$. We can now write

$$(6.9) \quad \begin{aligned} \psi_6(1) &= -2 - 2A + 2B\sqrt{-3} - 2A - 2B\sqrt{-3} \\ &= -2 - 4A \end{aligned}$$

and by (4.5)

$$(6.10) \quad p = \psi(\beta^1, \beta^2) \cdot \psi(\beta^5, \beta^4) = A^2 + 3B^2.$$

Combining (6.1), (6.3), and (6.9) we have

$$(6.11) \quad A_6(Q) = \begin{cases} -1 - 2A & p \equiv 7 \pmod{12} \\ -1 - 2A + 2x \cdot \chi(Q) & p \equiv 1 \pmod{12} \quad 3 \mid x \\ -1 - 2A - 2x \cdot \chi(Q) & p \equiv 1 \pmod{12} \quad 3 \nmid x. \end{cases}$$

Using Equation (3.7), Equation (6.9) can be written in the form

$$(6.12) \quad \psi_6(1) = 2\phi_3(1) = -2 - 4A.$$

Thus we have

$$(6.13) \quad \phi_3(1) = -1 - 2A.$$

Which corresponds to the result of Von Schrutka [8].

7. The evaluation of $A_{10}(Q)$. If $p = x^2 + 4y^2 = u^2 + 5v^2$, $A_{10}(Q)$ is expressed as a linear combination of u, X, U, V and W , where X, U, V , and W are solutions of the pair of diophantine equations

$$16p = X^2 + 50U^2 + 50V^2 + 125W^2 \quad \text{and} \quad XW = V^2 - 4UV - U^2.$$

Signs are selected so that $X \equiv 1 \pmod{5}$, and $u \equiv x \pmod{5}$ where $x \equiv 1 \pmod{4}$.

$p \not\equiv 1 \pmod{10}$. Brewer [2] has evaluated $A_5(Q)$, $Q \equiv m^2 \pmod{p}$, with the results

$$(7.1) \quad A_5(Q) = \begin{cases} -4u \cdot \chi(m) & p \equiv 1 \pmod{20} \ 5 \nmid x \\ 4u \cdot \chi(m) & p \equiv 9 \pmod{20} \ 5 \nmid x \\ 0 & \text{otherwise.} \end{cases}$$

These results together with the corollary to Theorem 5.6 gives us for $p \not\equiv 1 \pmod{10}$

$$(7.2) \quad A_{10}(Q) = \begin{cases} -1 + 4u \cdot \chi(Q) & p \equiv 9 \pmod{20} \ 5 \nmid x \\ -1 & \text{otherwise.} \end{cases}$$

$p \equiv 1 \pmod{10}$. Say $p = 10f + 1$. By Equation (5.9)

$$(7.3) \quad A_{10}(Q) = \chi(Q) \cdot A_5 + \frac{1}{2} \psi_{10}(1).$$

Whiteman [10] has expressed the cyclotomic numbers of order ten as linear combinations of p, X, U, V , and W , where X, U, V , and W are solutions of the pair of diophantine equations $16p = X^2 + 50U^2 + 50V^2 + 125W^2$ and $XW = V^2 - 4UV - U^2$ with $X \equiv 1 \pmod{5}$. However, rather than evaluating $\psi_{10}(1)$ directly from the cyclotomic numbers as was done with $\psi_6(1)$ in the case of $A_6(Q)$, it is more expeditions to use (4.12). Thus (7.3) becomes

$$(7.4) \quad A_{10}(Q) = \chi(Q) \cdot A_5(1) + 5(B(i, 1) - 2f)$$

where i is selected so that $4g^i \equiv 1 \pmod{p}$. Let $g^r \equiv 2 \pmod{p}$ then $g^{2r} \equiv 4 \pmod{p}$. Thus i is selected so that $2r + i \equiv 0 \pmod{p-1}$. Since $(B(i, 1))$ is periodic with respect to e , we may write $i \equiv -2r \pmod{e}$. Whiteman [11, p. 101] gives the following values for the $B(i, 1)$:

$$(7.5) \quad \begin{aligned} 5B(0, 1) &= p - 2 + X \\ 20B(1, 1) &= 4p - 8 - X + 10U + 20V + 25W \\ 20B(2, 1) &= 4p - 8 - X + 20U - 10V - 25W \\ 20B(3, 1) &= 4p - 8 - X - 20U + 10V - 25W \\ 20B(4, 1) &= 4p - 8 - X - 10U - 20V + 25W. \end{aligned}$$

Thus if $p \equiv 1 \pmod{10}$ we have the following values

$$(7.6) \quad A_{10}(Q) = \begin{cases} \chi(Q) \cdot A_5(1) - 1 + X & r \equiv 0 \pmod{5} \\ \chi(Q) \cdot A_5(1) + \frac{1}{4}(-4 - X - 20U + 10V - 25W) & r \equiv 1 \pmod{5} \\ \chi(Q) \cdot A_5(1) + \frac{1}{4}(-4 - X + 10U + 20V + 25W) & r \equiv 2 \pmod{5} \\ \chi(Q) \cdot A_5(1) + \frac{1}{4}(-4 - X - 10U - 20V + 25W) & r \equiv 3 \pmod{5} \\ \chi(Q) \cdot A_5(1) + \frac{1}{4}(-4 - X + 20U - 10V - 25W) & r \equiv 4 \pmod{5} \end{cases}$$

with the value of $A_5(1)$ from (7.1)

$$A_5(1) = \begin{cases} -4u & p \equiv 1 \pmod{20} \text{ and } 5 \nmid x \\ 0 & \text{otherwise.} \end{cases}$$

REFERENCES

1. B. W. Brewer, *On certain character sums*, Trans. Amer. Math. Soc. **99** (1961), 241-245.
2. ———, *On primers of the form $u^2 + 5v^2$* , Proc. Amer. Math. Soc. **17** (1966), 502-509.
3. L. E. Dickson, *Cyclotomy, higher congruences and Warings problem*, Amer. J. Math. **57** (1935), 391-424.
4. M. Hall, Jr., *A survey of difference sets*, Proc. Amer. Math. Soc. **7** (1956), 975-986.
5. H. Hasse, *Vorlesungen Über Zahlentheorie*, Berlin, Springer-Verlag, 1950.
6. E. Jacobsthal, *Über die Darstellung der Primzahlen der Form $4n + 1$ als summe zweier Quadrate*, J. Reine Angew. Math. **132** (1907), 238-245.
7. E. Lehmer, *On the number of solutions of $u^k + D = w^2 \pmod{p}$* , Pacific J. Math. **5** (1955), 103-118.
8. L. Von Schrutka, *Eine Beweis für die zerlegbarkeit der primzahlen Von der Form $6n + 1$ in enifaches und ein driefaches Quadrat*, J. Reine Angew. Math. **140** (1911), 252-265.
9. A. L. Whiteman, *Theorems analogous to Jacobsthal's theorem*, Duke Math. J. **16** (1949), 619-626.
10. ———, *Cyclotomy and Jacobsthal sums*, Amer. J. Math. **74** (1952) 89-99.
11. ———, *The cyclotomic numbers of order ten*, Proceedings of the symposia in Applied Mathematics, Vol. X, Combinatorial Analysis, 1960, 95-111.
12. ———, *The cyclotomic numbers of order twelve*, Acta Arith. **6** (1960), 53-75.
13. ———, *A theorem of Brewer on character sums*, Duke Math. J. **30** (1963), 545-552.
14. ———, *Theorems on Brewer and Jacobsthal sums. I*, Proceedings of symposia in Pure Mathematics, Vol. XIII, Number Theory, 1965, 49-55.
15. ———, *Theorems on Brewer and Jacobsthal sums, II*, Michigan Math. J. **12** (1965) 65-80.

Recieved August 8, 1966, and in revised form November 1, 1967. This research was supported in part by National Science Foundation Grant GP 3464.