THEOREMS ON BREWER AND JACOBSTHAL SUMS. II

Albert Leon Whiteman

1. INTRODUCTION

Let $V_n(x)$ be the polynomial determined by the recurrence relation

$$V_{n+2}(x) = xV_{n+1}(x) - V_n(x) \qquad (n = 1, 2, \cdots)$$

with $V_1(x) = x$, $V_2(x) = x^2 - 2$. In a recent paper [1], B. W. Brewer has defined the sum

$$\Lambda_n = \sum_{s=0}^{p-1} \chi(V_n(s)),$$

where $\chi(s)$ denotes the Legendre symbol (s/p) and p is an odd prime. It is easily verified that $\Lambda_1 = 0$, $\Lambda_2 = -1$. Brewer evaluated Λ_3, Λ_4, and Λ_5. For a summary of the results pertaining to Λ_3 and Λ_4, see Part I of the present paper [9].

The results for the sum $\Lambda_5 = \Sigma_{s=0}^{p-1} \chi(s(s^4 - 5s^2 + 5))$ are as follows.

If $p \equiv 3 \pmod 4$ or if $p \equiv \pm 2 \pmod 5$, then $\Lambda_5 = 0$.

If $p = 20f + 1 = u^2 + 5v^2 = x^2 + 4y^2$ with $x \equiv 1 \pmod 4$, then $\Lambda_5 = 0$ if $5 \mid x$, and $\Lambda_5 = -4u$ if $5 \nmid x$ and $u \equiv x \pmod 5$.

If $p = 20f + 9 = u^2 + 5v^2 = x^2 + 4y^2$ with $x \equiv 1 \pmod 4$, then $\Lambda_5 = 0$ if $5 \mid x$, and $\Lambda_5 = 4u$ if $5 \nmid x$ and $u \equiv x \pmod 5$.

Moreover, the following congruences modulo p hold:

$$(1.1) \qquad \binom{10f}{f}\binom{10f}{3f} \equiv 4u^2, \qquad \binom{10f}{f} \equiv \pm\binom{10f}{3f} \qquad (p = 20f + 1),$$

$$(1.2) \qquad \binom{10f+4}{f}\binom{10f+4}{3f+1} \equiv 4u^2, \qquad \binom{10f+4}{f} \equiv \pm\binom{10f+4}{3f+1} \qquad (p = 20f + 9).$$

Brewer bases his method for evaluating Λ_5 upon the congruences in (1.1) and (1.2). The purpose of the present paper is to derive the results for Λ_5 without employing these congruences. In Part I, which has been published elsewhere [9], the following theorems are established. Theorem 1 gives the value of Λ_5 when $p \equiv \pm 2 \pmod 5$. Theorem 2 gives the value of Λ_5 when $p = 20f + 1$. Theorem 3 is a statement of the two congruences in (1.1) together with a resolution of the ambiguous sign in the second congruence. Let $p = 20f + 1$ and put $p = x^2 + 4y^2$. Theorem 3 asserts that then the ambiguous sign is plus if $5 \nmid x$ and is minus if $5 \mid x$.

The theory of cyclotomy modulo a prime $p = ef + 1$ leads, for $e = 20$, to the case $p = 20f + 1$. The method of [9] is based on this theory and was suggested by Cauchy's

Received August 17, 1964.
This paper was supported in part by National Science Foundation grant G 24066.

proof [2] of (1.1). A basic tool in the argument is a lemma of Brewer (see Lemma 1 in the next section).

In Part II, which is now presented, a theory of cyclotomy modulo a prime $p = E(2f + 1) - 1$ is developed. For $E = 10$, this leads to the case $p = 20f + 9$ (see Section 4). The method involves the factorization formula (3.5), which expresses p as the product of two complex factors composed of (2E)th roots of unity.

The sum $\lambda(\beta^n)$ defined in Theorem 1 is an Eisenstein sum [3]. Its role is analogous to that of the Jacobi sum $\psi(\beta^m, \beta^n)$ discussed in [9]. The coefficient a_i in the expansion (3.10) of $\lambda(\beta^n)$ is analogous to the coefficient B(i, v) in the corresponding expansion of $\psi(\beta^{vn}, \beta^n)$ (compare formula (3.6) in [9]). For some properties of the numbers a_i, see Lemmas 3, 4, and 5 in Section 3. The sum λ_n defined in (3.27) resembles the sum $\psi_{m,n}$ defined in Part I [9, formula (3.19)]. The divisibility properties of λ_n are given in Lemma 6.

The main results in Section 4 are as follows. Theorem 2 gives the value of Λ_5 when $p = 20f + 9$. Theorem 3 is a statement of the two congruences in (1.2), together with a resolution of the ambiguous sign in the second congruence. Let $p = 20f + 9$, and put $p = x^2 + 4y^2$. Then Theorem 3 asserts that the ambiguous sign is plus if $5 \nmid x$ and is minus if $5 \mid x$.

2. TWO LEMMAS

Let p be an odd prime, and let γ denote a generator of the multiplicative group of the field $GF(p^2)$. For $\xi \in GF(p^2)$, put

$$\mathrm{tr}(\xi) = \xi + \xi^p, \tag{2.1}$$

so that $\mathrm{tr}(\xi) \in GF(p)$. If $\xi \neq 0$, let $\overline{\xi}$ be the unique solution of the equation $\xi\overline{\xi} = 1$. The number $\theta = \gamma^{p-1}$ satisfies $\theta^{p+1} = 1$ and therefore $\overline{\theta} = \theta^p$. Thus, for $n \geq 1$, $\mathrm{tr}(\theta^n) = \theta^n + \overline{\theta}^n$.

The following lemma of Brewer [1, Lemma 2] is fundamental.

LEMMA 1. *Put* $\theta = \gamma^{p-1}$. *Let the sums* $\Lambda_n, \Omega_n, \Theta_n$ *be defined by*

$$\Lambda_n = \sum_{s=0}^{p-1} \chi(V_n(s)), \qquad \Omega_n = \sum_{h=1}^{p-1} \chi(h^n + \overline{h}^n), \qquad \Theta_n = \sum_{k=1}^{p+1} \chi(\theta^{kn} + \overline{\theta}^{kn}). \tag{2.2}$$

Then

$$2\Lambda_n = \Omega_n + \Theta_n.$$

This lemma is proved both in [1] and in [9].

We shall also make use of the Jacobsthal sum [7]

$$\phi(n) = \sum_{h=0}^{p-1} \chi(h)\chi(h^2 + n). \tag{2.3}$$

The classical theorem of Jacobsthal [4] is the remarkable identity stated in the next lemma.

LEMMA 2. *Let* $p \equiv 1 \pmod 4$, *and let* N *be an integer such that* $\chi(N) = -1$. *Then*

$$p = \left(\frac{\phi(1)}{2}\right)^2 + \left(\frac{\phi(N)}{2}\right)^2,$$

where $\phi(1)/2 \equiv -1 \pmod 4$.

3. CYCLOTOMY modulo $p = E(2f + 1) - 1$

If γ is a primitive root of $GF(p^2)$, then $\gamma^{p+1} = g$ is a primitive root of $GF(p)$. For $\xi \in GF(p^2)$ $(\xi \neq 0)$, let ind ξ be the index of ξ to the base γ, defined modulo $p^2 - 1$ by means of the equation $\gamma^{\text{ind}\,\xi} = \xi$. Let $e \mid p^2 - 1$, and let $\beta = \exp(2\pi i/e)$ be a primitive eth root of unity. The Lagrange resolvent $\tau(\beta^n)$ over $GF(p^2)$ is defined by

$$\tau(\beta^n) = \sum_{\xi \in GF(p^2)} \beta^{n\,\text{ind}\,\xi} \zeta^{\text{tr}(\xi)}, \tag{3.1}$$

where $\zeta = \exp(2\pi i/p)$ and the summation extends over all numbers of $GF(p^2)$ except 0. By a theorem of Stickelberger [6, p. 335] we see that

$$\tau(\beta^n)\,\tau(\beta^{-n}) = \beta^{n\,\text{ind}\,(-1)}\,p^2, \tag{3.2}$$

if n is an integer not divisible by e. It is easy to construct a proof of (3.2) similar to the proof of the corresponding result in $GF(p)$ (see the proof of Satz 979 in [5]).

Let N be a quadratic nonresidue of p. The polynomial $P(x) = x^2 - N$ is irreducible in the finite field $GF(p)$ of residues modulo p. Hence the residues $a + bx$ $(a, b \in GF(p))$ modulo $P(x)$ form a finite field $GF(p^2)$. In what follows it will be convenient to use this concrete representation of $GF(p^2)$.

The principal result of this section is given in the following theorem.

THEOREM 1. *Let* $E \mid p + 1$ *and put* $e = 2E$, *so that* $e \mid p^2 - 1$. *Suppose that* $(p + 1)/E$ *is odd, and put* $p + 1 = ef + E$. *Then the sum*

$$\lambda(\beta^n) = \sum_{b=0}^{p-1} \beta^{n\,\text{ind}\,(1+bx)} \tag{3.3}$$

has the properties

$$\lambda(\beta^n) = (-1)^{n/2+1} \quad (n \textit{ even}, e \nmid n), \tag{3.4}$$

$$\lambda(\beta^n)\lambda(\beta^{-n}) = p \quad (n \textit{ odd}). \tag{3.5}$$

Proof. It is convenient to introduce character notation. If $\xi \in GF(p^2)$, we put

$$\chi(\xi) = \begin{cases} \beta^{\text{ind}\,\xi} & (\xi \neq 0), \\ 0 & (\xi = 0). \end{cases}$$

Thus χ is an eth power character of $GF(p^2)$. We now write (3.3) in the alternate form

$$\lambda(\beta^n) = \sum_{b=0}^{p-1} \chi^n(1 + bx). \tag{3.6}$$

For $a \in GF(p)$ $(a \neq 0)$, put $g^j = a$. Then $\chi(a) = \beta^{(p+1)j} = (-1)^j$. This means that the character $\chi(a)$ reduces to the ordinary Legendre symbol (a/p). Thus, if $a \neq 0$, we have the relations

$$\sum_{b=0}^{p-1} \chi^n(1 + bx) = \chi^n(a) \sum_{b=0}^{p-1} \chi^n(a + abx) = \chi^n(a) \sum_{b=0}^{p-1} \chi^n(a + bx).$$

We next note the familiar result

$$\sum_{\xi \in GF(p^2)} \chi^n(\xi) = \begin{cases} p^2 - 1 & (e \mid n), \\ 0 & (e \nmid n). \end{cases} \tag{3.7}$$

Let $\xi = a + bx$, where $a, b \in GF(p)$. Then the left member of (3.7) becomes

$$\sum_{a=0}^{p-1} \sum_{b=0}^{p-1} \chi^n(a + bx) = \sum_{b=0}^{p-1} \chi^n(bx) + \sum_{a=1}^{p-1} \sum_{b=0}^{p-1} \chi^n(a + bx)$$

$$= \chi^n(x) \sum_{b=0}^{p-1} \chi^n(b) + \sum_{a=1}^{p-1} \chi^n(a) \sum_{b=0}^{p-1} \chi^n(1 + bx).$$

To prove (3.4), assume that n is even and $e \nmid n$. Then by (3.6) and (3.7) we get

$$(p - 1)\chi^n(x) + (p - 1)\lambda(\beta^n) = 0.$$

Since

$$\chi^n(x) = (\chi(x^2))^{n/2} = (\chi(N))^{n/2} = (-1)^{n/2},$$

the relation in (3.4) follows at once.

By (2.1), $\mathrm{tr}(a + bx) = 2a$. Expressing (3.1) in terms of characters, we have the equation

$$\tau(\beta^n) = \sum_{a,b=0}^{p-1} \chi^n(a + bx)\zeta^{2a} = \sum_{b=0}^{p-1} \chi^n(bx) + \sum_{a=1}^{p-1} \sum_{b=0}^{p-1} \chi^n(a + bx)\zeta^{2a}$$

$$= \chi^n(x) \sum_{b=0}^{p-1} \chi^n(b) + \sum_{a=1}^{p-1} \chi^n(a)\zeta^{2a} \sum_{b=0}^{p-1} \chi^n(1 + bx).$$

To prove (3.5), assume that n is odd. Then the last equation reduces to

$$\tau(\beta^n) = \chi(2)\, G\lambda(\beta^n), \tag{3.8}$$

where $G = \Sigma_{a=0}^{p-1} \chi(a)\zeta^a$ is the familiar Gauss sum. It is well known that $G^2 = \chi(-1)p$. In (3.8), replace n by $-n$. Then (3.2) yields (3.5). This completes the proof of the theorem.

The hypothesis of Theorem 1 will be assumed throughout the rest of this section. We remark that in the special case where $E = 4$ and $n = 1$, Theorem 1 reduces to a theorem of Eisenstein [3]; see also [8, Lemma 2].

In the application of Theorem 1 we shall require the additional relation

$$\lambda(\beta^n) = \lambda(\beta^{n(E-1)}) \qquad (p + 1 = ef + E). \tag{3.9}$$

To prove (3.9), let $\alpha = 1 + bx$, where $b \in GF(p)$. Then $\alpha^p = 1 - bx$. Hence

$$\sum_{b=0}^{p-1} \chi^n(1 - bx) = \sum_{\alpha} \chi^n(\alpha^p) = \sum_{\alpha} \chi^{pn}(\alpha) = \sum_{b=0}^{p-1} \chi^{(E-1)n}(1 + bx),$$

where the second and third summations extend over all $p\alpha$. Using (3.6), we obtain (3.9) at once.

In (3.3), collect the exponents of β that are in the same residue class modulo e. Then we may write

$$\lambda(\beta^n) = \sum_{i=0}^{e-1} a_i \beta^{ni}, \tag{3.10}$$

where a_i is the number of values of b ($b = 0, 1, \cdots, p - 1$) for which $\operatorname{ind}(1 + bx) \equiv i \pmod{e}$. The following lemma is analogous to Lemma 3 in [9].

LEMMA 3. *Let* $p + 1 = ef + E$ *with* $e = 2E$. *Then*

$$a_i + a_{i+E} = \begin{cases} 2f & (i = E/2), \\ 2f + 1 & (0 \leq i \leq E - 1,\ i \neq E/2). \end{cases} \tag{3.11}$$

Proof. For each $\xi = a + bx$ with $a, b \in GF(p)$ we define a mapping $\xi \to \sigma(\xi)$ as follows:

$$\sigma(\xi) = \begin{cases} 1 + \bar{a}bx & (a \neq 0,\ a\bar{a} = 1), \\ 0 & (a = 0). \end{cases}$$

It is evident from this definition that

$$2\xi = \operatorname{tr}(\xi)\,\sigma(\xi) \qquad (\operatorname{tr}(\xi) \neq 0). \tag{3.12}$$

If γ is a primitive root of $GF(p^2)$, then $k = (p + 1)/2$ is the only value of k in the interval $1 \leq k \leq p + 1$ for which $\sigma(\gamma^k) = 0$. We now show that the set of p numbers

$$\sigma(\gamma^k) \qquad (1 \leq k \leq p + 1,\ k \neq (p + 1)/2)$$

is a permutation of the set of p numbers

$$1 + bx \qquad (b = 0, 1, \cdots, p - 1).$$

Assume the contrary. Let m, n be two integers such that $\sigma(\gamma^m) = \sigma(\gamma^n)$ with

$$1 \leq m, n \leq p + 1, \quad m \neq (p + 1)/2, \quad n \neq (p + 1)/2, \quad m \neq n.$$

If we put $\gamma^m = a + bx$ and $\gamma^n = c + dx$, then we get $\gamma^m = a\bar{c}\gamma^n$. Since $k = p + 1$ is the smallest positive integer such that $\gamma^k \in GF(p)$, we have a contradiction.

The coefficient a_i in (3.10) may now be defined as the number of values of k $(1 \leq k \leq p + 1, k \neq (p + 1)/2)$ for which $\operatorname{ind} \sigma(\gamma^k) \equiv i \pmod{e}$. Let $0 \leq i \leq E - 1$. If $k \equiv i \pmod{E}$ and $k \neq (p + 1)/2$, then $\operatorname{ind} \sigma(\gamma^k)$ is congruent to i or to $i + E \pmod{e}$; if $k = (p + 1)/2$, then $k \equiv E/2 \pmod{E}$ and $\sigma(\gamma^k) = 0$. Since $p + 1 = E(2f + 1)$ the interval $1 \leq k \leq p + 1$ contains $2f + 1$ integers k such that $k \equiv i \pmod{E}$. Consequently

$$a_i + a_{i+E} = \begin{cases} 2f & (i = E/2), \\ 2f + 1 & (i \neq E/2). \end{cases}$$

This establishes (3.11) and completes the proof of the lemma.

The coefficient a_i in (3.10) has been defined as the number of values of b $(b = 0, 1, \cdots, p - 1)$ for which $\operatorname{ind}(1 + bx) \equiv i \pmod{e}$. Formula (3.13) in the next lemma provides another means for determining a_i.

LEMMA 4. *Let* $p + 1 = ef + E$. *Let* γ *be a primitive root of* $GF(p^2)$, *and put* $\theta = \gamma^{p-1}$. *Let* b_i $(0 \leq i \leq e - 1)$ *denote the number of integers* k $(1 \leq k \leq p + 1, k \neq (p + 1)/2)$ *such that* $\operatorname{ind}(\theta^k + 1) \equiv i \pmod{e}$. *Then*

$$(3.13) \qquad a_i = \begin{cases} b_i & (\chi(2) = 1, \ i \text{ even; or } \chi(2) = -1, \ i \text{ odd}), \\ b_{i+E} & (\chi(2) = 1, \ i \text{ odd; or } \chi(2) = -1, \ i \text{ even}). \end{cases}$$

Proof. By (2:1) we have the equation

$$(3.14) \qquad \operatorname{tr}(\theta^k + 1) = (\theta^k + 1)(\bar{\theta}^k + 1).$$

Therefore the only value of k in the interval $1 \leq k \leq p + 1$ for which $\operatorname{tr}(\theta^k + 1) = 0$ is $k = (p + 1)/2$. Hence $\sigma(\theta^k + 1) \neq 0$ if $1 \leq k \leq p + 1$ and $k \neq (p + 1)/2$. Moreover, since

$$(\theta^k + 1)^p = \theta^{kp} + 1 = \theta^{p-k+1}(\theta^k + 1),$$

it follows that

$$(3.15) \qquad (\theta^k + 1)^{p-1} = \theta^{p-k+1} \qquad (1 \leq k \leq p + 1, \ k \neq (p + 1)/2).$$

We now assert that the set of p numbers

$$\sigma(\theta^k + 1) \qquad (1 \leq k \leq p + 1, \ k \neq (p + 1)/2)$$

is a permutation of the set of p numbers

$$1 + bx \qquad (b = 0, 1, \cdots, p - 1).$$

Assume the contrary. Let m, n be two integers such that $\sigma(\theta^m + 1) = \sigma(\theta^n + 1)$ with

$$1 \leq m, n \leq p + 1, \quad m \neq (p + 1)/2, \quad n \neq (p + 1)/2, \quad m \neq n.$$

If we put $\theta^m + 1 = a + bx$ and $\theta^n + 1 = c + dx$, then $\theta^m + 1 = a\bar{c}(\theta^n + 1)$. Raising both members of the last equation to the $(p - 1)$st power, we get, in view of (3.15), $\theta^{p-m+1} = \theta^{p-n+1}$ and hence $m = n$. This contradiction proves the assertion.

We have just established that the coefficient a_i in (3.10) is the number of integers k $(1 \leq k \leq p + 1, k \neq (p + 1)/2)$ such that $\chi(\sigma(\theta^k + 1)) = \beta^i$. On the other hand, b_i in Lemma 4 is the number of integers k $(1 \leq k \leq p + 1, k \neq (p + 1)/2)$ such that $\chi(\theta^k + 1) = \beta^i$. It remains to show that a_i is related to b_i by means of (3.13).

From the relation $\gamma\theta = \gamma^p$ we deduce that $\mathrm{tr}(\gamma^k) = \gamma^k(\theta^k + 1)$. This leads to the formula

$$\chi(\theta^k + 1) = \beta^{(e-1)k}\chi(\mathrm{tr}(\gamma^k)) \qquad (1 \leq k \leq p + 1). \tag{3.16}$$

If $k = (p + 1)/2$, both members of (3.16) vanish; otherwise, $\chi(\mathrm{tr}(\gamma^k)) = \pm 1$. Consequently,

$$\chi^2(\theta^k + 1) = \beta^{(e-2)k} \qquad \text{if } k \neq (p + 1)/2.$$

Now write (3.14) in the form $\mathrm{tr}(\theta^k + 1) = \bar{\theta}^k(\theta^k + 1)^2$. Since $\chi(\bar{\theta}^k) = \beta^{(E+2)k}$, it follows that

$$\chi(\mathrm{tr}(\theta^k + 1)) = (-1)^k \qquad (1 \leq k \leq p + 1, k \neq (p + 1)/2). \tag{3.17}$$

Next take $\xi = \theta^k + 1$ in (3.12). Making use of (3.17), we get

$$\chi(\sigma(\theta^k + 1)) = (-1)^k\chi(2)\chi(\theta^k + 1) \qquad (1 \leq k \leq p + 1). \tag{3.18}$$

We note that both sides of (3.18) vanish for $k = (p + 1)/2$.

Finally, let $0 \leq i \leq E - 1$. By (3.16), if $k \equiv E - i \pmod{E}$ and $k \neq (p + 1)/2$, then $\chi(\theta^k + 1)$ has one of the values β^i and β^{E+i}, and $k \equiv i \pmod 2$. As an immediate consequence of (3.18), we may now deduce (3.13). The proof of the lemma is thus complete.

We return to the sum Θ_n defined in (2.2). Our object is to express this sum in terms of the coefficients a_i. For this purpose it is convenient to introduce the related sum

$$\Theta_n(i) = \sum_{k=1}^{p+1} \chi(\theta^{i+kn} + 1) \qquad (1 \leq i \leq p + 1). \tag{3.19}$$

Note that if the integer n is such that $\chi(\theta^n) = 1$, then $\Theta_n = \Theta_{2n}(0)$.

For $p + 1 = ef + E$, we have the relation $\chi(\theta^n) = \beta^{(E-2)n}$, so that $\chi(\theta^n) = 1$ if $(E - 2)n \equiv 0 \pmod e$. In particular,

$$\chi(\theta^n) = 1 \text{ if } \begin{cases} E \equiv 2 \pmod 4 \text{ and } n = E/2, & \text{or} \\ E \equiv 0 \pmod 4 \text{ and } n = E. \end{cases}$$

Thus, if $E \equiv 2 \pmod 4$, then $\Theta_{E/2} = \Theta_E(0)$. Again, if $E \equiv 0 \pmod 4$, then $\Theta_E = \Theta_{2E}(0)$. We also note that $\Theta_{2E}(0) = \Theta_E(0)$, since the set of numbers $2E, 4E, \cdots, 2(p+1)E$ modulo $p+1$ is a permutation of the set of numbers $E, 2E, \cdots, (p+1)E$ modulo $p+1$. In summary,

$$\Theta_E(0) = \begin{cases} \Theta_E & (E \equiv 0 \pmod 4), \\ \Theta_{E/2} & (E \equiv 2 \pmod 4). \end{cases} \tag{3.20}$$

It should be noted that, in view of (3.16), each term of the sum $\Theta_E(0)$ has the value ± 1. Consequently, $\Theta_E(0)$ can be written in the form $E(A - B)$, where A is the number of times that the symbol $\chi(\theta^{Ek} + 1)$ $(1 \leq k \leq 2f + 1)$ takes the value 1, and B is the number of times that it takes the value -1. Since $p + 1$ is not divisible by e, there is no value of k $(1 \leq k \leq 2f + 1)$ for which $\chi(\theta^{Ek} + 1)$ takes the value 0. It follows that $p + 1 = E(A + B)$, and hence $\Theta_E(0)$ can be expressed as follows:

$$\Theta_E(0) = -p - 1 + eA \qquad (p + 1 = ef + E). \tag{3.21}$$

The next lemma furnishes a formula for evaluating $\Theta_E(i)$.

LEMMA 5. *If* $p + 1 = ef + E$, *then*

$$\Theta_E(i) = -\chi(2)E(a_i - a_{i+E})\beta^{E-i} \qquad (0 \leq i \leq E - 1). \tag{3.22}$$

Proof. We shall make use of the identity

$$\Theta_E(i) = \beta^{(E-2)i}\Theta_E(E - i) \qquad (0 \leq i \leq E - 1), \tag{3.23}$$

which may be established in the following manner:

$$\chi(\theta^{E-i}) \sum_{k=1}^{p+1} \chi(\theta^{Ek+i} + 1) = \sum_{k=1}^{p+1} \chi(\theta^{Ek+E} + \theta^{E-i})$$

$$= \sum_{k=1}^{p+1} \chi(\theta^{-Ek} + \theta^{E-i}) = \sum_{k=1}^{p+1} \chi(\theta^{Ek+E-i} + 1).$$

Since $\theta^{p+1} = \theta^{E(2f+1)} = 1$, we may also write

$$\Xi - i) = \sum_{k=1}^{p+1} \chi(\theta^{Ek+E-i} + 1) = E \sum_{k=1}^{2f+1} \chi(\theta^{Ek+E-i} + 1).$$

For $i = E/2$ and $k = f$, we have the identity $\chi(\theta^{Ek+E-i} + 1) = 0$. Otherwise, (3.16) implies that each term in the last sum is equal to β^i or β^{i+E}. In view of the definition of b_i in Lemma 4, the sum reduces to $(b_i - b_{i+E})\beta^i$. Introducing this result into (3.23), we get

$$\Theta_E(i) = E(b_i - b_{i+E})\beta^{(E-1)i} \qquad (0 \leq i \leq E-1). \tag{3.24}$$

With the aid of Lemma 4, it is easy to verify that (3.22) is equivalent to (3.24). This completes the proof of the lemma.

We now establish the following corollary of Lemma 5.

COROLLARY. *Let* $p+1 = ef+E$. *If* $E \equiv 0 \pmod 4$, *then*

$$\Theta_E = (-1)^{E/4} E(a_0 - a_E). \tag{3.25}$$

If $E \equiv 2 \pmod 4$, *then*

$$\Theta_{E/2} = \begin{cases} (-1)^f E(a_0 - a_E) & (E \equiv 2 \pmod 8), \\ (-1)^{f+1} E(a_0 - a_E) & (E \equiv 6 \pmod 8). \end{cases} \tag{3.26}$$

Proof. If $E \equiv 0 \pmod 4$, then

$$p \equiv \begin{cases} -1 \pmod 8 & \text{if } E \equiv 0 \pmod 8, \\ 3 \pmod 8 & \text{if } E \equiv 4 \pmod 8. \end{cases}$$

Hence $\chi(2) = (-1)^{E/4}$. By (3.20), $\Theta_E = \Theta_E(0)$. For $i = 0$, (3.22) reduces to (3.25). If $E \equiv 2 \pmod 4$, then

$$p \equiv \begin{cases} 4f+1 \pmod 8 & \text{if } E \equiv 2 \pmod 8, \\ 4f-3 \pmod 8 & \text{if } E \equiv 6 \pmod 8. \end{cases}$$

Hence $\chi(2) = (-1)^f$ if $E \equiv 2 \pmod 8$ and $\chi(2) = (-1)^{f+1}$ if $E \equiv 6 \pmod 8$. By (3.20), $\Theta_{E/2} = \Theta_E(0)$. For $i = 0$, (3.22) becomes (3.26). This completes the proof of the corollary.

We now return to the sum $\lambda(\beta^n)$ in (3.10). Put $F = (p^2-1)/e$. Then the number e is the smallest positive integer such that $\beta^e = 1$ and $\gamma^{eF} = 1$ in $GF(p^2)$. Thus it is natural to define the sum

$$\lambda_n = \sum_{b=0}^{p-1} (1+bx)^{nF}. \tag{3.27}$$

This means that $\lambda(\beta^n)$ becomes λ_n when β is replaced by γ^F.

The number λ_n has useful divisibility properties. We shall derive the following lemma.

LEMMA 6. *Let* $p+1 = ef+E$. *For* $0 < n < e$, *the number* λ_n *satisfies*

(i) $\lambda_n \equiv (-1)^{n/2+1} \pmod p$ (n *even*),

(ii) $\lambda_n \equiv 0 \pmod p$ ($0 < n < E$, n *odd*),

(iii) $\lambda_n \equiv \chi(2)\binom{(p-1)/2}{p-nf-(n-1)/2} \pmod p$ ($E < n < e$, n *odd*).

Proof. The number $F = (p^2 - 1)/e$ may also be written in the form

$$F = (p + E - 1)f + (E - 2)/2 .$$

It follows that the exponent nF in (3.27) can be expressed in the following manner:

$$nF = z + wp ,$$

where

$$z = \begin{cases} (e - 2j)f + E - 1 - j & (n = 2j), \\ (E - 2j - 1)f + (E - 2)/2 - j & (0 < n < E,\ n = 2j + 1), \\ (3E - 2j - 1)f + (3E - 4)/2 - j & (E < n < e,\ n = 2j + 1), \end{cases}$$

and

$$w = \begin{cases} 2jf + j - 1 & (n = 2j), \\ (2j + 1)f + j & (0 < n < E,\ n = 2j + 1), \\ (2j + 1)f + j - 1 & (E < n < e,\ n = 2j + 1). \end{cases}$$

Hence (3.27) becomes

$$\lambda_n = \sum_{b=0}^{p-1} (1 + bx)^z (1 + bx)^{wp} = \sum_{b=0}^{p-1} (1 + bx)^z (1 - bx)^w$$

$$= \sum_{r=0}^{z} \sum_{s=0}^{w} \binom{z}{r} \binom{w}{s} (-1)^s x^{r+s} \sum_{b=0}^{p-1} b^{r+s}$$

For each pair r, s in the triple sum,

$$0 \le r + s \le z + w = \begin{cases} p - 1 & (n = 2j), \\ (p - 1)/2 & (0 < n < E,\ n = 2j + 1), \\ 3(p - 1)/2 & (E < n < e,\ n = 2j + 1). \end{cases}$$

Cases (i) and (ii) of the lemma are now readily established: Since

$$\sum_{b=0}^{p-1} b^m \equiv \begin{cases} 0 \pmod p & (p - 1 \nmid m \text{ or } m = 0), \\ -1 \pmod p & (p - 1 \mid m \text{ and } m > 0), \end{cases}$$

the triple sum reduces to $(-1)^{n/2+1}$ modulo p in Case (i) and to 0 modulo p in Case (ii).

Case (iii) is more troublesome. Clearly it suffices to restrict the triple sum to those pairs r, s for which $r + s = p - 1$ and $p - 1 - w \le r \le z$. Since

(3.28) $$r!\,s! \equiv (-1)^{s+1} \pmod p \qquad (r + s = p - 1),$$

the triple sum reduces in this case to

$$\sum_{r=y}^{z} \binom{z}{r}\binom{w}{s}(-1)^{s+1} x^{p-1} = -\sum_{r=y}^{z} \frac{z!\,w!}{(z-r)!\,(w-s)!},$$

where $y = p - 1 - w = (e - 2j - 1)f + E - j - 1$. We next put $P = (p - 1)/2$, $r = y + t$, $s = w - t$, where $0 \le t \le P$. This yields

$$\lambda_n = -\frac{z!\,w!}{P!}\sum_{t=0}^{P} \frac{P!}{(P-t)!\,t!} = -\frac{z!\,w!}{P!}\,2^P.$$

Making three applications of (3.28), we obtain the equation

$$\lambda_n = -\chi(2)\,\frac{P!}{(p-1-z)!\,(p-1-w)!}\,(-1)^{z+w+P+3} = \chi(2)\binom{P}{y},$$

which is equivalent to the result in Case (iii) of the lemma.

4. THE CASE $p = 20f + 9$

For $p + 1 = ef + E$ with $e = 20$ and $E = 10$, the number β is a primitive twentieth root of unity. Thus $\beta^8 = \beta^6 - \beta^4 + \beta^2 - 1$. The equation (3.10) becomes

(4.1) $$\lambda(\beta^n) = \sum_{i=0}^{19} a_i \beta^{ni},$$

where a_i is the number of values of b ($b = 0, 1, \cdots, p - 1$) for which

$$\operatorname{ind}(1 + bx) \equiv i \pmod{20}.$$

Putting $d_i = a_i - a_{i+10}$ ($i = 0, 1, \cdots, 9$) and applying (4.1) with $n = 1$ and $n = 9$, we get

(4.2) $$\lambda(\beta) = \sum_{j=0}^{4} (d_{4j} - d_8)\beta^{4j} + \sum_{j=0}^{4} (d_{4j+1} - d_9)\beta^{4j+1},$$

(4.3) $$\lambda(\beta^9) = \sum_{j=0}^{4} (d_{16j} + d_2)\beta^{4j} + \sum_{j=0}^{4} (d_{16j+9} - d_1)\beta^{4j+1}.$$

We shall prove that both (4.2) and (4.3) lead to a representation of p in the form $u^2 + 5v^2$.

By (3.9), $\lambda(\beta) = \lambda(\beta^9)$. Equating coefficients of like powers of β in (4.2) and (4.3), we deduce the relations $d_1 = d_9$, $d_2 = -d_8$, $d_3 = d_7$, $d_4 = -d_6$. Therefore

$$(4.4)\qquad \begin{aligned} &a_1 - a_{11} = a_9 - a_{19}, \quad a_3 - a_{13} = a_7 - a_{17}, \\ &a_2 - a_{12} = -(a_8 - a_{18}), \quad a_4 - a_{14} = -(a_6 - a_{16}). \end{aligned}$$

Also, by Lemma 3,

$$(4.5)\qquad \begin{aligned} &a_0 + a_{10} = a_2 + a_{12} = a_4 + a_{14} = a_6 + a_{16} = a_8 + a_{18} = 2f + 1, \\ &a_1 + a_{11} = a_3 + a_{13} = a_7 + a_{17} = a_9 + a_{19} = 2f + 1, \quad a_5 + a_{15} = 2f. \end{aligned}$$

Combining (4.4) and (4.5), we find that

$$(4.6)\qquad \begin{aligned} &a_1 = a_9, \quad a_2 = a_{18}, \quad a_3 = a_7, \quad a_4 = a_{16}, \\ &a_6 = a_{14}, \quad a_8 = a_{12}, \quad a_{11} = a_{19}, \quad a_{13} = a_{17}. \end{aligned}$$

It is convenient to put $\eta = \beta^{16}$. Then $1 + \eta + \eta^2 + \eta^3 + \eta^4 = 0$. Using (4.4) and (4.5), we now transform (4.2) as follows:

$$\begin{aligned} \lambda(\beta) &= [2a_0 - 2f - 1 - (2a_2 - 2f - 1)(\eta^2 + \eta^3) + (2a_4 - 2f - 1)(\eta + \eta^4)] \\ &\quad + [2a_5 - 2f - (2a_3 - 2f - 1)(\eta^2 + \eta^3) + (2a_1 - 2f - 1)(\eta + \eta^4)]\beta^5 \\ &= [2a_0 + a_2 - a_4 - 2f - 1 + (a_2 + a_4 - 2f - 1)(\eta - \eta^2 - \eta^3 + \eta^4)] \\ &\quad + [2a_5 + a_3 - a_1 - 2f + (a_3 + a_1 - 2f - 1)(\eta - \eta^2 - \eta^3 + \eta^4)]\beta^5 . \end{aligned}$$

This yields the first of the following four equations.

$$(4.7)\qquad \begin{cases} \lambda(\beta^9) = a + b\beta^5 + (c + d\beta^5)(\eta - \eta^2 - \eta^3 + \eta^4), \\ \lambda(\beta^{11}) = a - b\beta^5 + (c - d\beta^5)(\eta - \eta^2 - \eta^3 + \eta^4), \\ \lambda(\beta^7) = a - b\beta^5 - (c - d\beta^5)(\eta - \eta^2 - \eta^3 + \eta^4), \\ \lambda(\beta^{13}) = a + b\beta^5 - (c + d\beta^5)(\eta - \eta^2 - \eta^3 + \eta^4), \end{cases}$$

where

$$(4.8)\qquad \begin{cases} a = -1 + 2a_0 + a_2 - a_4 - 2f, \\ b = \quad 2a_5 + a_3 - a_1 - 2f, \\ c = \quad -1 + a_2 + a_4 - 2f, \\ d = \quad -1 + a_3 + a_1 - 2f. \end{cases}$$

The remaining three equations in (4.7) may be derived in a similar manner. Under the mapping $\beta \to \beta^{-1}$, the expression $\eta - \eta^2 - \eta^3 + \eta^4$ is invariant and the first equation in (4.7) goes into the second, while the third is carried into the fourth. Under the mapping $\beta \to \beta^3$ the expression $\eta - \eta^2 - \eta^3 + \eta^4$ goes into $-(\eta - \eta^2 - \eta^3 + \eta^4)$, and the first equation in (4.7) goes into the third. Clearly, $\lambda(\beta^{11})$ is the complex conjugate of $\lambda(\beta^9)$, and $\lambda(\beta^{13})$ is the complex conjugate of $\lambda(\beta^7)$. From (3.5) of Theorem 1, we deduce that

$$\lambda(\beta^9)\lambda(\beta^{11}) = p, \qquad \lambda(\beta^7)\lambda(\beta^{13}) = p.$$

It is easily verified that $(\eta - \eta^2 - \eta^3 + \eta^4)^2 = 5$. By (4.7), the product $\lambda(\beta^9)\lambda(\beta^{11})$ yields the equation

$$p = a^2 + b^2 + 5(c^2 + d^2) + 2(ac + bd)(\eta - \eta^2 - \eta^3 + \eta^4).$$

Since $\eta - \eta^2 - \eta^3 + \eta^4$ is irrational, the number $ac + bd$ must vanish. The last equation thus simplifies to

$$p = a^2 + b^2 + 5(c^2 + d^2) \quad \textit{with} \quad ac + bd = 0. \tag{4.9}$$

In order to obtain additional properties of a, b, c, d, it is expedient to replace the twentieth root of unity β by γ^F, where γ is a fixed primitive root of $GF(p^2)$ and $F = (p^2 - 1)/20$. In the notation of (3.27), $\lambda(\beta^n)$ becomes λ_n. Let the number $r = \gamma^{16F}$ correspond to $\eta = \beta^{16}$. Then the four equations in (4.7) are transformed into the four equations

$$\begin{cases} \lambda_9 = a + b\gamma^{5F} + (c + d\gamma^{5F})(r - r^2 - r^3 + r^4), \\ \lambda_{11} = a - b\gamma^{5F} + (c - d\gamma^{5F})(r - r^2 - r^3 + r^4), \\ \lambda_7 = a - b\gamma^{5F} - (c - d\gamma^{5F})(r - r^2 - r^3 + r^4), \\ \lambda_{13} = a + b\gamma^{5F} - (c + d\gamma^{5F})(r - r^2 - r^3 + r^4). \end{cases} \tag{4.10}$$

LEMMA 7. *The equation* (4.9) *reduces to one of the following two possibilities:*

(i) $p = b^2 + 5c^2$, $a = d = 0$,

(ii) $p = a^2 + 5d^2$, $b = c = 0$.

Proof. We first show that

$$c \textit{ and } d \textit{ cannot both equal zero.} \tag{4.11}$$

Otherwise, putting $c = d = 0$ in (4.9) and (4.10), we get $p = a^2 + b^2$ and

$$\lambda_{11}\lambda_{13} \equiv a^2 + b^2 \pmod{p}.$$

But the product $\lambda_{11}\lambda_{13}$ cannot be divisible by p, since Lemma 6 yields

$$\lambda_{11}\lambda_{13} \equiv \binom{10f+4}{f}\binom{10f+4}{3f+1} \pmod{p}.$$

This contradiction proves (4.11).

We next show that $ab = 0$. If $ab \neq 0$, put $-c/b = d/a = k$. Equation (4.9) becomes $p = (a^2 + b^2)(1 + 5k^2)$. If $a^2 + b^2 = 1$, then $a = 0$ and $b = \pm 1$, or $a = \pm 1$ and $b = 0$. If $1 + 5k^2 = 1$, then $k = c = d = 0$, in violation of (4.11). This proves that $ab = 0$. Finally, if $a = 0$ and $d \neq 0$, or if $b = 0$ and $c \neq 0$, then (4.9) implies that $5 \mid p$, an impossibility. The proof of the lemma is thus complete.

We shall also require a representation of p in the form $x^2 + 4y^2$. Returning to (4.1), we take $n = 5$ and obtain

$$\lambda(\beta^5) = \sum_{j=0}^{4} (a_{4j} - a_{4j+2}) + \beta^5 \sum_{j=0}^{4} (a_{4j+1} - a_{4j+3}). \tag{4.12}$$

It is clear that the complex conjugate of $\lambda(\beta^5)$ is $\lambda(\beta^{-5})$. We now put (compare [9, formula (4.12)])

$$(-1)^f \lambda(\beta^5) = x + 2y\beta^5. \tag{4.13}$$

From (3.5) it follows that $p = x^2 + 4y^2$. Equating real and imaginary parts in (4.12) and (4.13), we get

$$(-1)^f x = (a_0 + a_4 + a_8 + a_{12} + a_{16}) - (a_2 + a_6 + a_{10} + a_{14} + a_{18}),$$

$$(-1)^f 2y = (a_1 + a_5 + a_9 + a_{13} + a_{17}) - (a_3 + a_7 + a_{11} + a_{15} + a_{19}).$$

With the aid of (4.4) and (4.5), we can simplify the last two equations to

$$\begin{cases} (-1)^f x = -1 + 2a_0 - 4(a_2 - a_4) - 2f, \\ (-1)^f 2y = \quad 2a_5 - 4(a_3 - a_1) - 2f. \end{cases} \tag{4.14}$$

We next show that $a_0 \equiv 1 \pmod 2$, whence $x \equiv 1 \pmod 4$. The value of x in (4.13) is thereby precisely determined by the equation

$$p = x^2 + 4y^2 \quad \textit{with } x \equiv 1 \pmod 4. \tag{4.15}$$

To prove that a_0 is odd, we employ Lemma 5 with E = 10. Using (4.5), we obtain

$$\Theta_{10}(0) = (-1)^f 10(-1 + 2a_0 - 2f). \tag{4.16}$$

Hence it suffices to show that $\Theta_{10}(0) \equiv 10 \pmod{40}$.

From (3.21), we get

$$\Theta_{10}(0) = -p - 1 + 20A, \tag{4.17}$$

where A is the number of values of k ($k = 1, 2, \cdots, 2f + 1$) for which $\chi(\theta^{10k} + 1)$ takes the value 1. If $k = 2f + 1$, then $\chi(\theta^{10k} + 1) = \chi(2) = (-1)^f$. For $k = 1, 2, \cdots, 2f$, group the integers k into pairs so that k and $2f + 1 - k$ form a pair. By (3.14) and (3.17),

$$\chi(\theta^{10k} + 1) = \chi(\theta^{10(2f+1-k)}) \qquad (1 \leq k \leq 2f).$$

Therefore A is even or odd according as f is odd or even. In either event, (4.17) implies that $\Theta_{10}(0) \equiv 10 \pmod{40}$. This proves the assertion that a_0 is odd.

It is instructive to compare the formulas for a, b, c, d in (4.8) with the formulas for x, y in (4.14). Suppose that a = 0. Then $(-1)^f x = -5(a_2 - a_4)$, so that $5 \mid x$. Conversely, suppose that $5 \mid x$. In the proof of Lemma 7 it is shown that if $a \neq 0$, then b = 0. Hence $(-1)^f 2y = -5(a_3 - a_1)$, so that $5 \mid y$. But $5 \mid x$ together with $5 \mid y$ implies $5 \mid p$, an impossibility. We conclude that a = 0 if and only if $5 \mid x$. The following improved formulation of Lemma 7 is an immediate consequence.

LEMMA 8. *Let* $p = 20f + 9 = x^2 + 4y^2$. *If* $5 \mid x$, *then* $a = d = 0$ *and* $p = b^2 + 5c^2$. *If* $5 \nmid x$, *then* $b = c = 0$ *and* $p = a^2 + 5d^2$.

On the one hand, Lemma 8 expresses p in the form $u^2 + 5v^2$ with $u = a + b$ and $u^2 = a^2 + b^2$. On the other hand, the lemma expresses a and b ambiguously in terms of u. In fact, if $p = u^2 + 5v^2$, then $a = 0$ and $b = u$ when $5 \mid x$, and $a = u$ and $b = 0$ when $5 \nmid x$. We now show how to remove the ambiguity in the sign of u in case $5 \nmid x$. Comparing the formula for a in (4.8) with the formula for x in (4.14), we see that $a \equiv (-1)^f x \pmod 5$. In view of (4.15), the sign of x is determined by the condition $x \equiv 1 \pmod 4$. Consequently, if we henceforth put $u = (-1)^f a$ when $5 \nmid x$, then the condition $u \equiv x \pmod 5$ with $x \equiv 1 \pmod 4$ will be satisfied.

We now establish the following theorem.

THEOREM 2. *Let* $p = 20f + 9 = u^2 + 5v^2 = x^2 + 4y^2$, *with* $x \equiv 1 \pmod 4$. *If* $5 \nmid x$, *let* u *be uniquely determined by* $u \equiv x \pmod 5$. *Then*

$$\sum_{s=0}^{p-1} \chi(s(s^4 - 5s^2 + 5)) = \begin{cases} 0 & (5 \mid x), \\ 4u & (5 \nmid x). \end{cases}$$

Proof. The sum in Theorem 2 is Λ_5. By Lemma 1, $2\Lambda_5 = \Omega_5 + \Theta_5$. Since $p \not\equiv 1 \pmod 5$, the sum Ω_5 reduces to the Jacobsthal sum $\phi(1)$ defined in (2.3). By (3.20), $\Theta_5 = \Theta_{10}(0)$. Hence $2\Lambda_5 = \phi(1) + \Theta_{10}(0)$. We now show that

$$\phi(1) = -2x, \qquad \Theta_{10}(0) = 2x + (-1)^f 8a. \tag{4.17}$$

The first equation in (4.17) follows from Lemma 2. The second equation in (4.17) is a consequence of (4.16). Using (4.8) and (4.14), we can easily verify that the right member of (4.16) is equal to $2x + (-1)^f 8a$. From (4.17) we obtain $2\Lambda_5 = (-1)^f 8a$. In view of the discussion following the statement of Lemma 8, it is clear that $a = 0$ if $5 \mid x$ and that $a = (-1)^f u$ if $5 \nmid x$. This proves Theorem 2.

The next theorem eliminates the ambiguity in the second congruence of (1.2).

THEOREM 3. *Let* $p = 20f + 9 = u^2 + 5v^2 = x^2 + 4y^2$. *Then*

$$\binom{10f+4}{f}\binom{10f+4}{3f+1} \equiv 4u^2 \pmod p.$$

Furthermore,

$$\binom{10f+4}{f} \equiv \binom{10f+4}{3f+1} \text{ or } -\binom{10f+4}{3f+1} \pmod p,$$

according as $5 \nmid x$ *or* $5 \mid x$.

Proof. In the first place, it follows from (4.10) that

$$\begin{cases} \lambda_9 + \lambda_{13} = 2(a + b\gamma^{5F}), \\ \lambda_{11} + \lambda_7 = 2(a - b\gamma^{5F}). \end{cases}$$

In the second place, by Lemma 6,

$$\begin{cases} \lambda_9 + \lambda_{13} \equiv \chi(2) \binom{10f+4}{3f+1} \pmod{p}, \\ \lambda_{11} + \lambda_7 \equiv \chi(2) \binom{10f+4}{f} \pmod{p}. \end{cases}$$

In view of Lemma 8, $u^2 = a^2 + b^2$. This implies the first part of Theorem 3. Again, by Lemma 8, $a = 0$ if $5 \mid x$ and $b = 0$ if $5 \nmid x$. This implies the second part of Theorem 3.

REFERENCES

1. B. W. Brewer, *On certain character sums*, Trans. Amer. Math. Soc. 99 (1961), 241-245.
2. A. Cauchy, *Mémoire sur la théorie des nombres*, Oeuvres Complètes (1) 3 (1911), 5-83.
3. G. Eisenstein, *Zur Theorie der quadratischen Zerfällung der Primzahlen* $8n + 3$, $7n + 2$ *und* $7n + 4$, J. Reine Angew. Math. 37 (1848), 97-126.
4. E. Jacobsthal, *Über die Darstellung der Primzahlen der Form* $4n + 1$ *als Summe zweier Quadrate*, J. Reine Angew. Math. 132 (1907), 238-245.
5. E. Landau, *Vorlesungen über Zahlentheorie*, Vol. 3, S. Hirzel, Leipzig, 1927.
6. L. Stickelberger, *Über eine Verallgemeinerung der Kreisteilung*, Math. Ann. 37 (1890), 321-367.
7. A. L. Whiteman, *Cyclotomy and Jacobsthal sums*, Amer. J. Math. 74 (1952), 89-99.
8. ———, *A theorem of Brewer on character sums*, Duke Math. J. 30 (1963), 545-552.
9. ———, *Theorems on Brewer and Jacobsthal sums. I*, Proceedings of Symposia in Pure Mathematics, Vol. VIII, Number Theory, American Mathematical Society, (in press).

University of Southern California
Los Angeles, California