ON CERTAIN CHARACTER SUMS

BY

B. W. BREWER

1. **Introduction.** The character sums

$$\Phi_k(Q) = \sum_{x=0}^{p-1} \chi(x(x^k + Q)) \quad \text{and} \quad \psi_k(Q) = \sum_{x=0}^{p-1} \chi(x^k + Q),$$

where $\chi(f(x)) = (f(x) \mid p)$, have been studied. The connection of $\Phi_2(Q)$ and $\psi_3(Q)$ with the representations $p = a^2 + b^2$ ($a \equiv 1 \pmod 4$) and $p = s^2 + 3t^2$ ($s \equiv 1 \pmod 3$) of an odd prime p was established by Jacobsthal [4] and von Schrutka [6]. It follows from the results of Jacobsthal that $\Phi_2(1)$ has the value $-2a$ or 0 according as $p = a^2 + b^2$ or $p \neq a^2 + b^2$, and from the results of von Schrutka that $\psi_3(1)$ has the value $-2s$ or 0 according as $p = s^2 + 3t^2$ or $p \neq s^2 + 3t^2$. (An elegant development of these particular results is given in [3].) If $p = 8k+1 = c^2 + 2d^2$ ($c \equiv (-1)^{k+1} \pmod 4$), Whiteman [7] has shown that $\Phi_4(1) = 4c$. However, if $p = 8k+3 = c^2 + 2d^2$, $\Phi_4(1) = 0$. We shall establish a theorem for primes of the form $c^2 + 2d^2$ entirely similar to the results of Jacobsthal and von Schrutka mentioned above, and indicate some results obtained for primes of the form $u^2 + 5v^2$.

If p is a prime of the form $a^2 + b^2$ (b even) and Q is a quadratic nonresidue of p, Jacobsthal showed that $\Phi_2(Q) = \pm 2b$, but was unable to remove the ambiguity in sign for any specific choice of the nonresidue Q. E. Lehmer [5] has determined the sign of $\Phi_2(2)$ if p is a prime of the form $8n+5$. We shall determine the sign of $\Phi_2(-3)$ if p is of the form $12n+5$, and for these same primes, obtain a congruence defining b similar to one given by Stern for primes of the form $8n+5$.

2. **Three lemmas.** If $GF(p^m)$ denotes the finite field of p^m elements (p prime), then the following lemma is evident.

LEMMA 1. *If p is an odd prime, θ a nonzero element of $GF(p^m)$, and θ is of multiplicative period e, then for s a positive integer*

$$\sum_{k=0}^{e-1} \theta^{ks} = \begin{cases} e \text{ if } s \equiv 0 \pmod e, \\ \dfrac{\theta^{es} - 1}{\theta^s - 1} = 0 \text{ if } s \not\equiv 0 \pmod e. \end{cases}$$

This paper has been submitted to and accepted for publication by the Proceedings of the American Mathematical Society. It has been transferred to these Transactions, with the consent of the author, for technical reasons.

Presented to the Society, November 17, 1956 under the title *On certain character sums and related congruences*; received by the editors May 9, 1960 and, in revised form, August 1, 1960.

If P is an integer, and P^2-4 is a quadratic nonresidue of the odd prime p, the multiplicative period e of a root θ of $y^2-Py+1=0$ in $GF(p^2)$ is greater than 2 and divides $p+1$. Conversely, if the multiplicative period e of an element θ of $GF(p^2)$ is greater than 2 and divides $p+1$, then for some integer P, θ is a root of $y^2-Py+1=0$ with P^2-4 a quadratic nonresidue of p. If P is an integer, and P^2-4 is a quadratic residue of p, $y^2-Py+1=0$ has a root in $GF(p)$.

Let θ and θ^{-1} be the roots of $y^2-Py+1=0$ in $GF(p^2)$. Then $V_n=\theta^n+\theta^{-n}$ $(n=1, 2, \cdots)$ satisfy the recursive relation $V_{n+2}=PV_{n+1}-V_n$ and are elements of $GF(p)$, or what is equivalent, residues modulo p. From these remarks, we have

LEMMA 2. *Let p be an odd prime, ω and θ elements of $GF(p^2)$, ω of multiplicative period $p-1$ and θ of multiplicative period $p+1$. Let $V_1(x)=x$, $V_2(x)=x^2-2$, and $V_{n+2}(x)=xV_{n+1}(x)-V_n(x)$ $(n=1, 2, \cdots)$. Let*

$$\Lambda_n=\sum_{x=0}^{p-1}\chi(V_n(x)), \qquad \Omega_n=\sum_{h=1}^{p-1}\chi(\omega^{hn}+\omega^{-hn}), \quad \text{and} \quad \Theta_n=\sum_{h=1}^{p+1}\chi(\theta^{hn}+\theta^{-hn}).$$

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

Applying Euler's criterion to Ω_n and Θ_n in Lemma 2, we obtain

LEMMA 3. *Let ω, θ, and Λ_n be defined as in Lemma 2. Then*

$$2\Lambda_n=\sum_{s=0}^{(p-1)/2}\sum_{t=1}^{p-1}\binom{(p-1)/2}{s}\omega^{tn(p-4s-1)/2}+\sum_{s=0}^{(p-1)/2}\sum_{t=1}^{p+1}\binom{(p-1)/2}{s}\theta^{tn(p-4s-1)/2}$$

in $GF(p^2)$.

The application of these three lemmas to Λ_3, Λ_4, and Λ_5 leads to the results mentioned in the introduction. In making this application, the following congruences involving the binomial coefficients are needed.

If $p=4k+1=a^2+b^2$ $(a\equiv 1 \pmod 4)$,

$$\binom{2k}{k}\equiv 2a \pmod p \text{ (Gauss).} \tag{1}$$

If $p=8k+1=c^2+2d^2$ $(c\equiv(-1)^{k+1} \pmod 4)$,

$$\binom{4k}{k}\equiv -2c \pmod p \text{ (Gauss-Stern).} \tag{2}$$

If $p=8k+3=c^2+2d^2$ $(c\equiv(-1)^{k+1} \pmod 4)$,

$$\binom{4k+1}{k}\equiv 2c \pmod p \text{ (Stern-Eisenstein).} \tag{3}$$

If $p=20k+1=u^2+5v^2$,

$$(4)\qquad \binom{10k}{k}\binom{10k}{3k}\equiv 4u^2 \quad\text{and}\quad \binom{10k}{k}\equiv \pm\binom{10k}{3k} \pmod p \text{ (Cauchy).}$$

If $p=20k+9=u^2+5v^2$,

$$(5)\qquad \binom{10k+4}{k}\binom{10k+4}{3k+1}\equiv 4u^2 \text{ and } \binom{10x+4}{k}\equiv \pm\binom{10k+4}{3k+1} \pmod p.$$

The congruences in (5) can be obtained by combining the method of Cauchy [1] in obtaining (4) with that of Eisenstein [2] in obtaining (3).

3. Λ_3. We first prove

THEOREM 1. *If p is prime and $p=12k+5=a^2+b^2$ ($a\equiv 1 \pmod 4$), then $\Phi_2(-3)=2b$, where $b\equiv a \pmod 3$.*

Proof. We note that $\Lambda_3=\Phi_2(-3)$, and Lemma 2 gives $2\Phi_2(-3)=\Omega_3+\Theta_3$. Since $(3, p-1)=1$, we have $\Omega_3=\sum_{x=1}^{p-1}\chi(x^3+x^{-3})=\sum_{x=1}^{p-1}\chi(x+x^{-1})=\Phi_2(1)=-2a$, where $a\equiv 1 \pmod 4$. Since $\Theta_3=3\sum_{h=1}^{(p+1)/3}\chi(\theta^{3h}+\theta^{-3h})$, $\Theta_3\equiv 0 \pmod 3$, and this gives $\Phi_2(-3)\equiv -a \pmod 3$, where $a\equiv 1 \pmod 4$. Then, -3 being a quadratic nonresidue of p, we have $\Phi_2(-3)=2b$, where $b\equiv a \pmod 3$ ($a\equiv 1 \pmod 4$), and Theorem 1 is proved.

Continuing under the hypothesis of Theorem 1, we now apply Lemma 3 and then Lemma 1 to $\Lambda_3=\Phi_2(-3)$. Noting that ω^{-1} has the same multiplicative period as ω, and θ^{-1} has the same multiplicative period as θ, we obtain

$$\begin{aligned}2\Phi_2(-3) &\equiv (p-1)\binom{6k+2}{3k+1}+2(p+1)\binom{6k+2}{k}+(p+1)\binom{6k+2}{3k+1}\\ &\equiv 2\binom{6k+2}{k} \pmod p.\end{aligned}$$

Then applying Theorem 1, we have

THEOREM 2. *If p is prime and $p=12k+5=a^2+b^2$ ($a\equiv 1 \pmod 4$), then*

$$\binom{6k+2}{k}\equiv 2b \pmod p,$$

where $b\equiv a \pmod 3$.

4. Λ_4. We employ $\Lambda_4=\sum_{x=0}^{p-1}\chi(x^4-4x^2+2)$ to prove

THEOREM 3. *An odd prime p can be expressed in the form $p=c^2+2d^2$ if and only if $p=8k+1$ or $p=8k+3$. Moreover,*

$$\sum_{x=0}^{p-1}\chi((x+2)(x^2-2))=\begin{cases}0 \text{ if } p\neq c^2+2d^2,\\ 2c \ (c\equiv(-1)^{k+1} \pmod 4) \text{ if } p=c^2+2d^2.\end{cases}$$

Proof. The first part of the theorem is well known. To prove the second part, we apply Lemma 3 and then Lemma 1 to Λ_4.

If $p=8k-1$, we obtain

$$2\Lambda_4 \equiv 2(p-1)\binom{4k-1}{0} \pmod{p},$$

and hence $\Lambda_4 \equiv -1 \pmod{p}$.

If $p=8k-3$, we obtain

$$2\Lambda_4 \equiv 2(p-1)\binom{4k-2}{0} + (p-1)\binom{4k-2}{2k-1} + (p+1)\binom{4k-2}{2k-1} \pmod{p},$$

and hence $\Lambda_4 \equiv -1 \pmod{p}$.

If $p=8k+1$, we obtain

$$2\Lambda_4 \equiv 2(p-1)\binom{4k}{0} + 2(p-1)\binom{4k}{k} + (p-1)\binom{4k}{2k} + (p+1)\binom{4k}{2k} \pmod{p},$$

and then applying (2) we have $\Lambda_4 \equiv 2c-1 \bmod p$, where $c \equiv (-1)^{k+1} \pmod 4$.

If $p=8k+3$, we obtain

$$2\Lambda_4 \equiv 2(p-1)\binom{4k+1}{0} + 2(p+1)\binom{4k+1}{k} \pmod{p},$$

and then applying (3) we have $\Lambda_4 \equiv 2c-1 \pmod{p}$, where $c \equiv (-1)^{k+1} \pmod 4$. Now

$$\sum_{x=0}^{p-1}\chi((x+2)(x^2-2)) = \sum_{x=0}^{p-1}\chi(x(x^2-4x+2)) = \sum_{x=0}^{p-1}[1+\chi(x)][\chi(x^2-4x+2)]$$
$$- \sum_{x=0}^{p-1}\chi(x^2-4x+2) = \sum_{x=0}^{p-1}\chi(x^4-4x^2+2)+1 = \Lambda_4+1.$$

Therefore

$$(6)\quad \sum_{x=0}^{p-1}\chi((x+2)(x^2-2)) \equiv \begin{cases} 0 \pmod p & \text{if } p=8k-1 \text{ or } p=8k-3, \\ 2c \pmod p & \text{if } p=8k+1 \text{ or } p=8k+3, \end{cases}$$

where $c \equiv (-1)^{k+1} \pmod 4$. Since the sum on the left in (6) is even and numerically less than p, (6) implies

$$\sum_{x=0}^{p-1}\chi((x+2)(x^2-2)) = \begin{cases} 0 & \text{if } p=8k-1 \text{ or } p=8k-3, \\ 2c & \text{if } p=8k+1 \text{ or } p=8k+3, \end{cases}$$

where $c \equiv (-1)^{k+1} \pmod 4$, and Theorem 3 is proved.

We note that Theorem 3 for the case $p=8k+1$ is also implied by the result of Whiteman mentioned in the introduction since then

$$2\sum_{x=0}^{p-1}\chi((x+2)(x^2-2)) = 2\Lambda_4 + 2 = \Omega_4 + \Theta_4 + 2 = \psi_8(1) + 2a + 1$$
$$= \Phi_4(1) + \Phi_2(1) + \psi_2(1) + 2a + 1 = \Phi_4(1) = 4c.$$

5. Λ_5. The proof of Theorem 3 suggests a similar application of our lemmas to $\Lambda_5 = \sum_{x=0}^{p-1}\chi(x(x^4-5x^2+5))$, the relevant congruences now being (1), (4), and (5). This yields a result similar to Theorem 3, but less complete. We omit the details of the proof but state the result as

THEOREM 4. *Let p be an odd prime. If $p \neq u^2 + 5v^2$, then $p = 20k + r$ ($r=3, 7, 11, 13, 17,$ or 19), and*

$$\sum_{x=0}^{p-1}\chi(x(x^4 - 5x^2 + 5)) = 0.$$

If $p=u^2+5v^2$, then either $p=20k+1=a^2+b^2$ ($a\equiv 1 \pmod 4$), and

$$\sum_{x=0}^{p-1}\chi(x(x^4 - 5x^2 + 5)) = \begin{cases} 0 & \text{if } a \equiv 0 \pmod 5, \\ -4u & (u \equiv a \pmod 5) \text{ if } a \not\equiv 0 \pmod 5, \end{cases}$$

or $p=20k+9=a^2+b^2$ ($a\equiv 1 \pmod 4$), and

$$\sum_{x=0}^{p-1}\chi(x(x^4 - 5x^2 + 5)) = \begin{cases} 0 & \text{if } a \equiv 0 \pmod 5, \\ 4u & (u \equiv a \pmod 5) \text{ if } a \not\equiv 0 \pmod 5. \end{cases}$$

REMARK. It would be interesting to obtain proofs of Theorems 3 and 4 independent of congruences involving the binomial coefficients. The congruences (2) and (3) would then follow as corollaries to Theorem 3. Several proofs of (2) have been given, but as far as the writer knows, the proof of (3) given by Eisenstein is the only one appearing in the literature.

REFERENCES

1. A. Cauchy, *Oeuvres complètes*, series 1, vol. 3, 1911, pp. 5–37.

2. G. Eisenstein, *Zur Theorie der quadratischen Zerfällung der Primzahlen $8n+3$, $7n+2$ und $7n+4$*, J. Reine Angew. Math. vol. 37 (1848) pp. 97–126.

3. H. Hasse, *Vorlesungen über Zahlentheorie*, Berlin, Springer-Verlag, 1950.

4. E. Jacobsthal, *Anwendungen einer Formel aus der Theorie der quadratischen Reste*, Dissertation, University of Berlin, 1906.

5. E. Lehmer, *On the number of solutions of $u^k+D\equiv w^2 \pmod p$*, Pacific J. Math. vol. 5 (1955) pp. 103–118.

6. L. von Schrutka, *Eine Beweis für die Zerlegbarkeit der Primzahlen von der Form $6n+1$ in ein einfaches und ein dreifaches Quadrat*, J. Reine Angew. Math. vol. 140 (1911) pp. 252–265.

7. A. L. Whiteman, *Theorems analogous to Jacobsthal's theorem*, Duke Math. J. vol. 16 (1949) pp. 619–626.

THE AGRICULTURAL AND MECHANICAL COLLEGE OF TEXAS,
COLLEGE STATION, TEXAS