PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 73, Number 3, March 1979

EVALUATION OF CHARACTER SUMS CONNECTED WITH ELLIPTIC CURVES

KENNETH S. WILLIAMS[1]

ABSTRACT. Let p be an odd prime and let $(\frac{\cdot}{p})$ be the Legendre symbol. It is shown how to evaluate the character sum $\sum_{x=0}^{p-1}(\frac{f(x)}{p})$, for certain quartic polynomials $f(x)$. For example, it is shown that

$$\sum_{x=0}^{p-1}\left(\frac{x^4-8x^3+12x^2-16x+4}{p}\right) = \begin{cases} 2\left(\frac{2}{p}\right)x_1 - 1, & \text{if } p \equiv 1 \pmod 4, \\ -1, & \text{if } p \equiv 3 \pmod 4, \end{cases}$$

where x_1 is defined for primes $p \equiv 1 \pmod 4$ by

$$p = x_1^2 + y_1^2, \quad x_1 \equiv -1 \pmod 4.$$

Let p be an odd prime and let $(\frac{\cdot}{p})$ be the Legendre symbol. It was shown in [28] (by completely elementary means) that, if F is a complex-valued function defined on the integers, which is periodic with period p, then

$$\sum_{x=0}^{p-1}{}' F\left(\frac{ax^2+bx+c}{Ax^2+Bx+C}\right) = \sum_{x=0}^{p-1} F(x) + \sum_{x=0}^{p-1}\left(\frac{Dx^2+\Delta x+d}{p}\right)F(x) - \begin{cases} F(a/A), & \text{if } A \not\equiv 0 \pmod p, \\ 0, & \text{if } A \equiv 0 \pmod p, \end{cases} \tag{1}$$

where a, b, c, A, B, C are integers; D, Δ, d are defined by

$$D = B^2 - 4AC, \quad \Delta = 4aC - 2bB + 4cA, \quad d = b^2 - 4ac;$$

and

$$\Delta^2 - 4Dd = 16\{(aC-cA)^2 - (aB-bA)(bC-cB)\} \not\equiv 0 \pmod p.$$

The prime ($'$) in (1) indicates that the summation excludes terms for which $Ax^2+Bx+C \equiv 0 \pmod p$. Note that at least one of a, A is nonzero $(\bmod\, p)$; that if $A \equiv B \equiv 0 \pmod p$ then $C \not\equiv 0 \pmod p$; that if $aB - bA \equiv$

Received by the editors January 16, 1978 and, in revised form, May 13, 1978.

AMS (MOS) subject classifications (1970). Primary 10G05; Secondary 14K22, 10D25.

Key words and phrases. Legendre symbol, character sums, elliptic curves, complex multiplication.

[1]Research supported under National Research Council of Canada Grant A-7233.

$0 \pmod p$ then $aC - cA \not\equiv 0 \pmod p$; and that $ax^2 + bx + c$ and $Ax^2 + Bx + C$ do not have a common root $(\bmod p)$.

It is the purpose of this note to show how (1) can be used to evaluate the character sum $\sum_{x=0}^{p-1}\left(\frac{f(x)}{p}\right)$, for certain quartic polynomials $f(x)$. First we take $F(x) = \left(\frac{x}{p}\right)$ in (1). As $\sum_{x=0}^{p-1}\left(\frac{x}{p}\right) = 0$, we obtain

$$\sum_{x=0}^{p-1}\left(\frac{(ax^2+bx+c)(Ax^2+Bx+C)}{p}\right)$$
$$= \sum_{x=0}^{p-1}\left(\frac{x(Dx^2+\Delta x+d)}{p}\right) - \left(\frac{aA}{p}\right). \tag{2}$$

If we choose a, b, c, A, B, C so that $y^2 = x^3 + \Delta x^2/D + dx/D$ is an elliptic curve over Q with complex multiplication, then

$$\sum_{x=0}^{p-1}\left(\frac{x(Dx^2+\Delta x+d)}{p}\right)$$

can be evaluated explicitly using Deuring's theorem **[9]**. The sum

$$\sum_{x=0}^{p-1}\left(\frac{(ax^2+bx+c)(Ax^2+Bx+C)}{p}\right)$$

can then be evaluated using (2). (For Deuring's theorem applied to the evaluation of character sums, see for example **[16]**, **[17]**, **[20]**, **[21]**, and for lists of elliptic curves with complex multiplication, see **[10]**, **[22]**.) We give some examples.

EXAMPLE 1. The elliptic curve E_1 given by $y^2 = x^3 + kx$ has complex multiplication by $\sqrt{-1}$. Writing $\operatorname{End}(E_1)$ for the ring of endomorphisms of E_1, we have in this case

$$\operatorname{End}(E_1) = Z + Z(\sqrt{-1}) \qquad [\mathbf{10}].$$

The corresponding character sum

$$\sum_{x=0}^{p-1}\left(\frac{x^3+kx}{p}\right) = \sum_{x=0}^{p-1}\left\{1+\left(\frac{x}{p}\right)\right\}\left(\frac{x^2+k}{p}\right) - \sum_{x=0}^{p-1}\left(\frac{x^2+k}{p}\right)$$
$$= \sum_{x=0}^{p-1}\left(\frac{x^4+k}{p}\right) + 1 \quad (p \nmid 2k)$$

was first treated by Jacobsthal **[12]** and later, from various points of view, by other authors, see for example Berndt and Evans **[1]**, Burde **[4]**, Chowla **[6]**, Davenport and Hasse **[8]**, Lehmer **[13]**, Morlaye **[15]**, Rajwade **[19]**, Singh and Rajwade **[24]**, Whiteman **[25]**, **[26]**. Some of these authors use only elementary methods (for example **[1]**, **[13]**), others do not (for example **[8]**, **[19]**). If $p \equiv 1 \pmod 4$ we define an integer x_1 uniquely by

$$p = x_1^2 + y_1^2, \quad x_1 \equiv -1 \pmod 4.$$

Then we have [**1**, Theorem 4.4]

$$\sum_{x=0}^{p-1}\left(\frac{x(x^2+k)}{p}\right)=\begin{cases}2\left(\frac{k}{p}\right)_4 x_1, & \text{if } p\equiv 1 \pmod 4,\quad \left(\frac{k}{p}\right)=1,\\ \pm 2y_1, & \text{if } p\equiv 1 \pmod 4,\quad \left(\frac{k}{p}\right)=-1,\\ 0, & \text{if } p\equiv 3 \pmod 4.\end{cases}$$

Hence, if $\Delta \equiv 0 \pmod p$, $d \equiv Dg^2 \not\equiv 0 \pmod p$, from (2) we have

$$\sum_{x=0}^{p-1}\left(\frac{(ax^2+bx+c)(Ax^2+Bx+C)}{p}\right)$$

$$=\begin{cases}2\left(\frac{Dg}{p}\right)x_1-\left(\frac{aA}{p}\right), & \text{if } p\equiv 1 \pmod 4,\\ -\left(\frac{aA}{p}\right), & \text{if } p\equiv 3 \pmod 4.\end{cases} \tag{3}$$

Let

$$a=t,\quad b=t+1,\quad c=1,$$
$$A=t+1,\quad B=2,\quad C=0,$$

where $t \not\equiv 0, \pm 1 \pmod p$. Then

$$d=(t-1)^2,\quad \Delta=0,\quad D=4,\quad g\equiv \pm\tfrac{1}{2}(t-1) \pmod p,$$

and (3) gives

$$\sum_{x=0}^{p-1}\left(\frac{x(x+1)(tx+1)((t+1)x+2)}{p}\right)$$

$$=\begin{cases}2\left(\frac{2(t-1)}{p}\right)x_1-\left(\frac{t(t+1)}{p}\right), & \text{if } p\equiv 1 \pmod 4,\\ -\left(\frac{t(t+1)}{p}\right), & \text{if } p\equiv 3 \pmod 4.\end{cases}$$

The special case $t=3$ gives the result (see Chowla [7])

$$\sum_{x=0}^{p-1}\left(\frac{6x^4+11x^3+6x^2+x}{p}\right)=\begin{cases}2\left(\frac{2}{p}\right)x_1-\left(\frac{6}{p}\right), & \text{if } p\equiv 1 \pmod 4,\\ -\left(\frac{6}{p}\right), & \text{if } p\equiv 3 \pmod 4.\end{cases}$$

EXAMPLE 2. The elliptic curve E_2 given by $y^2 = x^3 - 4kx^2 + 2k^2x$ has complex multiplication by $\sqrt{-2}$,

$$\mathrm{End}(E_2) = Z + Z(\sqrt{-2}) \qquad [\mathbf{10}].$$

The sum

$$\sum_{x=0}^{p-1}\left(\frac{x^3-4kx^2+2k^2x}{p}\right) \quad (p \nmid 2k)$$

was first considered by Brewer [3] and later by other authors (some using only elementary methods), Berndt and Evans [2], Leonard and Williams [14], Rajwade [16], [20], Whiteman [27], Williams [30]. If $p \equiv 1$ or $3 \pmod 8$, we define an integer x_2 uniquely by

$$p = x_2^2 + 2y_2^2, \quad x_2 \equiv 2[p/8] - 1 \pmod 4.$$

Then we have [2, Theorems 5.12 and 5.17]

$$\sum_{x=0}^{p-1}\left(\frac{x(x^2-4kx+2k^2)}{p}\right) = \begin{cases} 2\left(\frac{k}{p}\right)x_2, & \text{if } p \equiv 1 \text{ or } 3 \pmod 8, \\ 0, & \text{if } p \equiv 5 \text{ or } 7 \pmod 8. \end{cases}$$

Hence, if $\Delta \equiv -4Dg \not\equiv 0 \pmod p$, $d \equiv 2Dg^2 \not\equiv 0 \pmod p$, from (2) we have

$$\sum_{x=0}^{p-1}\left(\frac{(ax^2+bx+c)(Ax^2+Bx+C)}{p}\right)$$

$$= \begin{cases} 2\left(\frac{Dg}{p}\right)x_2 - \left(\frac{aA}{p}\right), & \text{if } p \equiv 1 \text{ or } 3 \pmod 8, \\ -\left(\frac{aA}{p}\right), & \text{if } p \equiv 5 \text{ or } 7 \pmod 8. \end{cases} \tag{4}$$

Let t be such that $t \not\equiv 0 \pmod p$, and set

$$a = 1, \quad b = 2t, \quad c = -t^2,$$
$$A = 1, \quad B = t, \quad C = 0,$$

so that

$$d = 8t^2, \quad \Delta = -8t^2, \quad D = t^2, \quad g = 2.$$

Then, from (4), we have

$$\sum_{x=0}^{p-1}\left(\frac{(x^2+2tx-t^2)(x^2+tx)}{p}\right) = \begin{cases} 2\left(\frac{2}{p}\right)x_2 - 1, & \text{if } p \equiv 1 \text{ or } 3 \pmod 8, \\ -1, & \text{if } p \equiv 5 \text{ or } 7 \pmod 8. \end{cases}$$

EXAMPLE 3. The elliptic curve E_3 given by $y^2 = x^3 - 3kx^2 + 3k^2x$ has complex multiplication by $\frac{1}{2}(-1+\sqrt{-3})$,

$$\operatorname{End}(E_3) = Z + Z\left(\frac{-1+\sqrt{-3}}{2}\right) \quad [\mathbf{10}].$$

The sum

$$\sum_{x=0}^{p-1}\left(\frac{x^3-3kx^2+3k^2x}{p}\right)=\sum_{x=0}^{p-1}\left(\frac{x^3+k^3}{p}\right)$$

$$=\left(\frac{k}{p}\right)\sum_{x=0}^{p-1}\left(\frac{x^3+1}{p}\right)=\left(\frac{k}{p}\right)\left\{1+\sum_{x=0}^{p-1}\left(\frac{x(x^3+1)}{p}\right)\right\}\quad (p\nmid 3k)$$

was first treated by von Schrutka **[23]** (using only elementary arguments) and later by a number of other authors including Berndt and Evans **[1]**, Chowla **[5]**, Davenport and Hasse **[11]**, Lehmer **[13]**, Rajwade **[17]**, **[18]**, Whiteman **[25]**, **[26]**, Williams **[29]**. If $p\equiv 1 \pmod 3$, we define an integer x_3 uniquely by

$$p=x_3^2+3y_3^2,\quad x_3\equiv -1 \pmod 3.$$

Then we have ([**1**, Theorem 4.1] or [**17**, Theorem 1])

$$\sum_{x=0}^{p-1}\left(\frac{x(x^2-3kx+3k^2)}{p}\right)=\begin{cases}2\left(\frac{k}{p}\right)x_3, & \text{if } p\equiv 1 \pmod 3,\\ 0, & \text{if } p\equiv 2 \pmod 3.\end{cases}$$

Hence, if $\Delta\equiv -3Dg\not\equiv 0 \pmod p$, $d\equiv 3Dg^2\not\equiv 0 \pmod p$ from (2) we have

$$\sum_{x=0}^{p-1}\left(\frac{(ax^2+bx+c)(Ax^2+Bx+C)}{p}\right)$$

$$=\begin{cases}2\left(\frac{Dg}{p}\right)x_3-\left(\frac{aA}{p}\right), & \text{if } p\equiv 1 \pmod 3,\\ -\left(\frac{aA}{p}\right), & \text{if } p\equiv 2 \pmod 3.\end{cases}\tag{5}$$

Let $t\not\equiv 0 \pmod p$ and set

$$a=1,\quad b=4t,\quad c=t^2,$$
$$A=1,\quad B=2t,\quad C=0,$$

so that

$$d=12t^2,\quad \Delta=-12t^2,\quad D=4t^2,\quad g=1.$$

Then, from (5), we have

$$\sum_{x=0}^{p-1}\left(\frac{(x^2+4tx+t^2)(x^2+2tx)}{p}\right)=\begin{cases}2x_3-1, & \text{if } p\equiv 1 \pmod 3,\\ -1, & \text{if } p\equiv 2 \pmod 3.\end{cases}$$

EXAMPLE 4. The elliptic curve E_7 given by $y^2=x^3+21kx^2+112k^2x$ has complex multiplication by $\frac{1}{2}(-1+\sqrt{-7})$,

$$\mathrm{End}(E_7)=Z+Z\left(\tfrac{1}{2}(-1+\sqrt{-7})\right)\qquad [\mathbf{10}],[\mathbf{21}],[\mathbf{22}].$$

The corresponding character sum

$$\sum_{x=0}^{p-1}\left(\frac{x^3+21kx^2+112k^2x}{p}\right) \quad (p \nmid 42k)$$

has recently been evaluated by Rajwade [21] by appealing to Deuring's theorem. No elementary proof of Rajwade's result is known at this time.

If $p \equiv 1, 2$ or $4 \pmod 7$, we define an integer x_7 uniquely by

$$p = x_7^2 + 7y_7^2, \quad x_7 \equiv 6, 3, 5 \pmod 7 \text{ respectively.}$$

Rajwade proved

$$\sum_{x=0}^{p-1}\left(\frac{x(x^2+21kx+112k^2)}{p}\right) = \begin{cases} 2\left(\frac{k}{p}\right)x_7, & \text{if } p \equiv 1, 2 \text{ or } 4 \pmod 7, \\ 0, & \text{if } p \equiv 3, 5 \text{ or } 6 \pmod 7. \end{cases}$$

Hence, if $\Delta \equiv 21Dg \not\equiv 0 \pmod p$, $d \equiv 112Dg^2 \not\equiv 0 \pmod p$, from (2) we have

$$\sum_{x=0}^{p-1}\left(\frac{(ax^2+bx+c)(Ax^2+Bx+C)}{p}\right)$$

$$= \begin{cases} 2\left(\frac{Dg}{p}\right)x_7 - \left(\frac{aA}{p}\right), & \text{if } p \equiv 1, 2 \text{ or } 4 \pmod 7, \\ -\left(\frac{aA}{p}\right), & \text{if } p \equiv 3, 5 \text{ or } 6 \pmod 7. \end{cases} \tag{6}$$

Let $t \not\equiv 0 \pmod p$ and choose

$$a = 1, \quad b = 6t, \quad c = 2t^2,$$
$$A = 3, \quad B = 16t, \quad C = 0,$$

so that

$$d = 28t^2, \quad \Delta = -168t^2, \quad D = 256t^2, \quad g = -1/32.$$

Then, from (6), we have

$$\sum_{x=0}^{p-1}\left(\frac{(x^2+6tx+2t^2)(3x^2+16tx)}{p}\right)$$

$$= \begin{cases} 2\left(\frac{-2}{p}\right)x_7 - \left(\frac{3}{p}\right), & \text{if } p \equiv 1, 2 \text{ or } 4 \pmod 7, \\ -\left(\frac{3}{p}\right), & \text{if } p \equiv 3, 5 \text{ or } 6 \pmod 7. \end{cases}$$

We remark that similar examples follow using the elliptic curves **[10]**:

$$E_1' : y^2 = x^3 - 6kx^2 + k^2x, \quad \mathrm{End}(E_1') = Z + Z(2\sqrt{-1}),$$

$$E_3' : y^2 = x^3 - 6kx^2 - 3k^2x, \quad \mathrm{End}(E_3') = Z + Z(\sqrt{-3}),$$

$$E_7' : y^2 = x^3 - 42kx^2 - 7k^2x, \quad \mathrm{End}(E_7') = Z + Z(\sqrt{-7}),$$

as the defining cubic in each case has no constant term.

Finally we take

$$F(x) = \left(\frac{gx^2 + hx + k}{p} \right)$$

in (1), where $g \not\equiv 0 \pmod p$ and $h^2 - 4gk \not\equiv 0 \pmod p$. As

$$\sum_{x=0}^{p-1} \left(\frac{gx^2 + hx + k}{p} \right) = -\left(\frac{g}{p} \right),$$

we obtain

$$\sum_{x=0}^{p-1} \left(\frac{g(ax^2 + bx + c)^2 + h(ax^2 + bx + c)(Ax^2 + Bx + C) + k(Ax^2 + Bx + C)^2}{p} \right)$$

$$= \sum_{x=0}^{p-1} \left(\frac{(gx^2 + hx + k)(Dx^2 + \Delta x + d)}{p} \right)$$

$$+ \begin{cases} \left(\frac{gD}{p} \right) - \left(\frac{ga^2 + haA + kA^2}{p} \right), & \text{if } A \not\equiv 0 \pmod p, \\ 0, \quad \text{if } A \equiv 0 \pmod p, \quad B \not\equiv 0 \pmod p, \\ -\left(\frac{g}{p} \right), & \text{if } A \equiv 0 \pmod p, \quad B \equiv 0 \pmod p. \end{cases} \tag{7}$$

One can use (7) in conjunction with (3), (4), (5) or (6) to obtain further evaluations. We give three examples to illustrate the ideas, all of which were conjectured by B. C. Berndt and R. J. Evans (personal communication). The author would like to thank Professor Berndt for a helpful discussion in connection with the preparation of this note.

EXAMPLE 5. For $p > 2$ we have

$$\sum_{x=0}^{p-1} \left(\frac{x^4 - 8x^3 + 12x^2 - 16x + 4}{p} \right)$$

$$= \sum_{x=0}^{p-1} \left(\frac{(x^2 - 4x + 2)^2 - 8x^2}{p} \right)$$

$$= \sum_{x=0}^{p-1} \left(\frac{(x^2 + 8x + 8)(x^2 - 8)}{p} \right) \quad \text{(by (7))}$$

$$= \begin{cases} 2\left(\frac{2}{p} \right) x_1 - 1, & \text{if } p \equiv 1 \pmod 4, \\ -1, & \text{if } p \equiv 3 \pmod 4 \end{cases} \quad \text{(by (3))}.$$

EXAMPLE 6. For $p > 3$ we have

$$\sum_{x=0}^{p-1}\left(\frac{x^4-8x^3+12x^2-8x+4}{p}\right)$$

$$=\sum_{x=0}^{p-1}\left(\frac{(x^2-4x+4)^2-12(x-1)^2}{p}\right)$$

$$=\sum_{x=0}^{p-1}\left(\frac{(x^2-12)(x^2+4x)}{p}\right) \quad \text{(by (7))}$$

$$=\begin{cases} 2x_3-1, & \text{if } p\equiv 1 \pmod 3, \\ -1, & \text{if } p \equiv 2 \pmod 3 \end{cases} \quad \text{(by (5))}.$$

EXAMPLE 7. For $p > 7$ we have

$$\sum_{x=0}^{p-1}\left(\frac{x^4-14x^3+63x^2-98x+21}{p}\right)$$

$$=\sum_{x=0}^{p-1}\left(\frac{(x^2-7x+7)^2-28}{p}\right)$$

$$=\sum_{x=0}^{p-1}\left(\frac{(-28x^2+1)(21x^2+4x)}{p}\right)+\left(\frac{-3}{p}\right)-1 \quad \text{(by (7))}$$

$$=\begin{cases} 2x_7-1, & \text{if } p\equiv 1,2,4 \pmod 7, \\ -1, & \text{if } p \equiv 3,5,6 \pmod 7 \end{cases} \quad \text{(by (6))}.$$

REFERENCES

1. Bruce C. Berndt and Ronald J. Evans, *Sums of Gauss, Jacobi, and Jacobsthal*, Rocky Mountain J. Math. (to appear).

2. ______, *Sums of Gauss, Eisenstein, Jacobi, Jacobsthal, and Brewer*, Illinois J. Math. (to appear).

3. B. W. Brewer, *On certain character sums*, Trans. Amer. Math. Soc. **99** (1961), 241–245.

4. Klaus Burde, *Über allgemeine Sequenzen der Länge 3 von Legendresymbolen*, J. Reine Angew. Math. **272** (1975), 203–216.

5. S. Chowla, *A formula similar to Jacobsthal's for the explicit value of x in* $p = x^2 + y^2$ *where p is a prime of the form* $4k + 1$, Proc. Lahore Philos. Soc. 7 (1945), 2 pp.

6. ______, *The last entry in Gauss's diary*, Proc. Nat. Acad. Sci. U.S.A. **35** (1949), 244–246.

7. ______, *On the class-number of the function-field* $y^2 = f(x)$ *over* $GF(p)$, Norske Vid. Selsk. Forh. **39** (1966), 86-88.

8. H. Davenport and H. Hasse, *Die Nullstellen der Kongruenzzetafuncktionen in gewissen zyklischen Fällen*, J. Reine Angew. Math. **172** (1934), 151–182.

9. M. Deuring, *Die Typen der Multiplikatorenringe elliptischer Funktionenkörper*, Abh. Math. Sem. Univ. Hamburg **14** (1941), 197–272.

10. Toshihiro Hadano, *Conductor of elliptic curves with complex multiplication and elliptic curves of prime conductor*, Proc. Japan Acad. **51** (1975), 92–95.

11. Helmut Hasse, *Vorlesgungen über Zahlentheorie*, Springer-Verlag, Berlin, 1964, pp. 158–166.

12. Ernst Jacobsthal, *Über die Darstellung der Primzahlen der Form* $4n + 1$ *als Summe zweier Quadrate*, J. Reine Angew. Math. **132** (1907), 238–245.

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

14. Philip A. Leonard and Kenneth S. Williams, *Jacobi sums and a theorem of Brewer*, Rocky Mountain J. Math. **5** (1975), 301–308; Erratum, Rocky Mountain J. Math. **6** (1976), 509.

15. B. Morlaye, *Démonstration élémentaire d'un théorème de Davenport et Hasse*, Enseignement Math. **8** (1972), 269–276.

16. A. R. Rajwade, *Arithmetic on curves with complex multiplication by* $\sqrt{-2}$, Proc. Cambridge Philos. Soc. **64** (1968), 659–672.

17. ______, *Arithmetic on curves with complex multiplication by the Eisenstein integers*, Proc. Cambridge Philos. Soc. **65** (1969), 59–73.

18. ______, *On rational primes p congruent to* 1 (mod 3 *or* 5), Proc. Cambridge Philos. Soc. **66** (1969), 61–70.

19. ______, *A note on the number* N_p *of the congruence* $y^2 \equiv x^3 - Dx \pmod p$, Proc. Cambridge Philos. Soc. **67** (1970), 603–605.

20. ______, *Certain classical congruences via elliptic curves*, J. London Math. Soc. (2) **8** (1974), 60–62.

21. ______, *The diophantine equation* $y^2 = x(x^2 + 21Dx + 112D^2)$ *and the conjectures of Birch and Swinnerton-Dyer*, J. Austral. Math. Soc. **24** (1977), 286–295.

22. ______, *Some formulae for elliptic curves with complex multiplication*, Indian J. Pure Appl. Math. (to appear).

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

24. Surjit Singh and A. R. Rajwade, *The number of solutions of the congruence* $y^2 \equiv x^4 - a \pmod p$, Enseignement Math. **20** (1974), 265–273.

25. Albert Leon Whiteman, *Theorems analogous to Jacobsthal's theorem*, Duke Math. J. **16** (1949), 619–626.

26. ______, *Cyclotomy and Jacobsthal sums*, Amer. J. Math. **74** (1952), 89–99.

27. ______, *A theorem of Brewer on character sums*, Duke Math. J. **30** (1963), 545–552.

28. Kenneth S. Williams, *Finite transformation formulae involving the Legendre symbol*, Pacific J. Math. **34** (1970), 559–568.

29. ______, *Note on a cubic character sum*, Aequationes Math. **12** (1975), 229–231.

30. ______, *Note on Brewer's character sum*, Proc. Amer. Math. Soc. **71** (1978), 153–154.

Department of Mathematics, Carleton University, Ottawa, Ontario, Canada K1S 5B6