



## Cubic Character Sums of Cubic Polynomials

David J. Wright

*Proceedings of the American Mathematical Society*, Vol. 100, No. 3. (Jul., 1987), pp. 409-413.

Stable URL:

<http://links.jstor.org/sici?sici=0002-9939%28198707%29100%3A3%3C409%3ACCSOCP%3E2.0.CO%3B2-V>

*Proceedings of the American Mathematical Society* is currently published by American Mathematical Society.

---

Your use of the JSTOR archive indicates your acceptance of JSTOR's Terms and Conditions of Use, available at <http://www.jstor.org/about/terms.html>. JSTOR's Terms and Conditions of Use provides, in part, that unless you have obtained prior permission, you may not download an entire issue of a journal or multiple copies of articles, and you may use content in the JSTOR archive only for your personal, non-commercial use.

Please contact the publisher regarding any further use of this work. Publisher contact information may be obtained at <http://www.jstor.org/journals/ams.html>.

Each copy of any part of a JSTOR transmission must contain the same copyright notice that appears on the screen or printed page of such transmission.

---

JSTOR is an independent not-for-profit organization dedicated to and preserving a digital archive of scholarly journals. For more information regarding JSTOR, please contact [support@jstor.org](mailto:support@jstor.org).

## CUBIC CHARACTER SUMS OF CUBIC POLYNOMIALS

DAVID J. WRIGHT

**ABSTRACT.** A complete evaluation is given of the sum over an arbitrary finite field of the values of a nontrivial cubic character of the field applied to an arbitrary polynomial of degree not greater than three in one variable defined over the field. Previous evaluations for the fields of prime order were given in theses of Friedman and Lagarias. The evaluation given below makes simple use of standard facts about equivalence of binary cubic forms. An interesting consequence of this evaluation is given connecting the values of these sums over the space of all polynomials of degree not greater than three over the finite field. The evaluation of these sums is of relevance to the theory of Shintani's Dirichlet series associated to the space of binary cubic forms since they appear in the residues of the cubic twists of these series.

**1. Introduction and summary of results.** Let  $\mathbf{F}_q$  be the finite field of prime power order  $q$ . We shall assume that  $q \equiv 1 \pmod{3}$ . Let  $\chi$  be a nontrivial character of the multiplicative group  $\mathbf{F}_q^\times$  of nonzero elements of  $\mathbf{F}_q$ . Extend  $\chi$  to  $\mathbf{F}_q$  by the convention  $\chi(0) = 0$ . To any  $x = (x_1, x_2, x_3, x_4)$  in the vector space  $V = \mathbf{F}_q^4$  we associate the polynomial

$$f_x(u) = x_1 u^3 + x_2 u^2 + x_3 u + x_4.$$

In this paper, we shall evaluate the sum  $S(\chi; x) = \sum_{u \in \mathbf{F}_q} \chi(f_x(u))$ . One special case of this sum is the Jacobi sum

$$J(\chi) = \sum_{u \in \mathbf{F}_q} \chi(u)\chi(1-u).$$

We shall see that all other sums  $S(\chi; x)$  may be simply expressed in terms of  $J(\chi)$ . Our method is centered upon the theory of binary cubic forms. To any  $x \in V$  we associate the form

$$F_x(u, v) = x_1 u^3 + x_2 u^2 v + x_3 u v^2 + x_4 v^3.$$

Define  $T(\chi; x) = \sum_{(u,v) \in \mathbf{F}_q^2} \chi(F_x(u, v))$ . A straightforward calculation shows that

$$(1.1) \quad T(\chi; x) = (q-1)\{S(\chi; x) + \chi(x_1)\}.$$

Let  $\Delta_x$  denote the discriminant of the form  $F_x$ , explicitly given by

$$(1.2) \quad \Delta_x = x_2^2 x_3^2 + 18x_1 x_2 x_3 x_4 - 4x_1 x_3^3 - 4x_2^3 x_4 - 27x_1^2 x_4^2.$$

The form  $F_x$  has multiple factors (i.e. is "singular") if and only if  $\Delta_x = 0$ . When  $\Delta_x \neq 0$ , define the function  $\lambda(x)$  to be 1 if the splitting field of  $F_x$  is  $\mathbf{F}_q$  or  $\mathbf{F}_{q^3}$  and to be  $-1$  if the splitting field is  $\mathbf{F}_{q^2}$ . If  $q$  is odd,  $\lambda(x)$  agrees with the quadratic symbol of  $\Delta_x$ . Our main result is as follows.

Received by the editors November 27, 1985, and in revised form, April 15, 1986.  
1980 *Mathematics Subject Classification* (1985 Revision). Primary 10G15.

**THEOREM 1.** For any  $x \in V$  with  $\Delta_x \neq 0$ ,

$$T(\chi; x) = (q - 1)\lambda(x)\chi(\Delta_x)J(\chi),$$

and

$$S(\chi; x) = -\chi(x_1) + \lambda(x)\chi(\Delta_x)J(\chi).$$

If  $\Delta_x = 0$ , then  $T(\chi; x) = 0$  unless  $f_x(u, v) = c(au + bv)^3$  for some  $c \neq 0$  and  $(a, b) \neq (0, 0)$ . In the latter case,  $T(\chi; x) = (q - 1)\chi(c)$ .

The sum  $T(\chi; x)$  may be further evaluated using explicit formulae for the Jacobi sums involved. The evaluation of  $J(\chi)$  is a venerable piece of number theory (see [2, 4]). We summarize the results as follows. Suppose  $q = p^n$  for some prime  $p$ . If  $p \equiv 1 \pmod 3$ , then

$$J(\chi) = (-1)^{n-1} \left( \frac{a + 3b\sqrt{-3}}{2} \right)^n,$$

where  $a$  and  $b$  are integers determined by the conditions  $a^2 + 27b^2 = 4p$  and  $a \equiv 1 \pmod 3$ . These requirements specify  $a$  and  $b$  up to the sign of  $b$  which depends on the precise choice of  $\chi$  versus  $\bar{\chi}$ . If  $p \equiv 2 \pmod 3$ , then  $n = 2m$  is even and  $J(\chi) = (-1)^{m-1}p^m$ . In all cases,  $|J(\chi)| = \sqrt{q}$ .

When  $q$  is a prime, this evaluation of  $S(\chi; x)$  was first given by Friedman [3], and later by Lagarias [5] using the theory of elliptic curves. Our method is substantially simpler. Moreover, we shall derive a striking consequence of Theorem 1 which we present below.

**THEOREM 2.**  $\sum_{x \in V} \bar{\chi}(\Delta_x)T(\chi; x) = 0$ .

As we shall see in the proof, this result does not arise from some argument based on orthogonality of characters, but instead requires explicit knowledge of the numbers of forms with given splitting fields.

Our interest in these sums was kindled by their appearance in the residues at  $s = \frac{5}{6}$  of the twists by cubic characters of Shintani's Dirichlet series associated to the space of binary cubic forms (see [1, 6]).

**2. Proofs.** Our proofs of Theorems 1 and 2 are founded on the theory of equivalence of binary cubic forms. For any  $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G = \text{Gl}_2(\mathbf{F}_q)$  and  $x \in V$ , we define  $g \cdot x \in V$  by the functional equation

$$F_{g \cdot x}(u, v) = \frac{1}{ad - bc} F_x(au + cv, bu + dv).$$

This is arranged so that  $\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \cdot x = ax$ . A basic feature of this representation is that

$$(2.1) \quad \Delta_{g \cdot x} = (\det g)^2 \Delta_x.$$

In fact, the discriminant generates the group of relative invariants of this representation of  $\text{Gl}_2$ .

The question of equivalence of binary cubic forms with coefficients in an arbitrary field  $K$  is analyzed by first factoring the form into three linear factors defined over an algebraic closure  $\bar{K}$  of  $K$ . In this way, we introduce the three "roots" of the binary cubic form. These roots are properly elements of the projective line  $\mathbf{P}^1(\bar{K})$ .

In the above representation, an element of  $GL_2$  acts on the roots of a binary cubic form as a linear fractional transformation. These facts are the key ingredients of the proofs of the following lemmas. The details for fields of zero characteristic are given in the remarks prior to Propositions 2.1, 2.2, and 2.3 in [7]. Since finite fields are perfect, the arguments presented there also suffice for this case.

LEMMA 1. *Two nonsingular binary cubic forms over  $F_q$  are  $G$ -equivalent if and only if their splitting fields are the same.*

The possible splitting fields over  $F_q$  are the extensions of degree not greater than three, namely,  $F_q$ ,  $F_{q^2}$ , and  $F_{q^3}$ . Thus, by Lemma 1, there are precisely three nonsingular  $G$ -orbits of forms.

LEMMA 2. *There are three singular  $G$ -orbits of binary cubic forms over  $F_q$ , with representatives  $(0, 0, 0, 0)$ ,  $(0, 0, 0, 1)$ , and  $(0, 0, 1, 0)$ .*

LEMMA 3. *The order of the stabilizer in  $G$  of nonsingular binary cubic forms with splitting field  $F_q$ ,  $F_{q^2}$ , and  $F_{q^3}$  is 6, 2, and 3, respectively.*

PROOF OF THEOREM 1. Since right multiplication by elements of  $G$  are automorphisms of  $F_q^2$ , we see that

$$T(\chi; g \cdot x) = \bar{\chi}(\det g)T(\chi; x).$$

In view of (2.1), we have

$$(2.2) \quad \bar{\chi}(\Delta_{g \cdot x})T(\chi; g \cdot x) = \bar{\chi}(\Delta_x)T(\chi; x).$$

We may also note that  $\lambda(g \cdot x) = \lambda(x)$  for all nonsingular  $x \in V$  and all  $g \in G$ . Consequently, we need merely verify either of the formulae of Theorem 1 for convenient representatives of all the  $G$ -orbits of forms. By Lemma 2, the singular orbits give rise to sums that are easily evaluated.

For the nonsingular orbits, let us first suppose that  $q$  is odd, that is, that  $q \equiv 1 \pmod 6$ . By Lemma 1 and the subsequent remarks, there are three nonsingular  $G$ -orbits with representatives:

$$x_I = (0, -1, 1, 0), \quad x_{II} = (0, r, 0, -1), \quad x_{III} = (s, 0, 0, -1),$$

where  $r$  is any element of  $F_q^\times$  that is not a square and  $s$  is any element that is not a cube. The existence of  $r$  and  $s$  follow from the hypothesis  $q \equiv 1 \pmod 6$ .

First, by definition, we have

$$S(\chi; x_I) = \sum_{u \in F_q} \chi(u - u^2) = J(\chi).$$

Noting that  $\Delta_{x_I} = 1$ , this result establishes Theorem 1 for  $x_I$  as well as all  $x$  in the  $G$ -orbit of  $x_I$ .

To handle  $x_{II}$ , we must introduce  $x'_{II} = (0, 1, 0, -1)$ . Since  $F_{x'_{II}}$  splits completely over  $F_q$ ,  $x_I$  and  $x'_{II}$  are  $G$ -equivalent. Thus, by (1.1), (1.2), and (2.2),

$$S(\chi; x'_{II}) = \frac{\chi(\Delta_{x'_{II}})}{\chi(\Delta_{x_I})} S(\chi; x_I) = \chi(4)J(\chi).$$

On the other hand, by partitioning  $\mathbf{F}_q$  into quadratic residues and nonresidues, we see that

$$S(\chi; x_{II}) + S(\chi; x'_{II}) = \sum_{u \in \mathbf{F}_q} \chi(ru^2 - 1) + \sum_{u \in \mathbf{F}_q} \chi(u^2 - 1) = 2 \sum_{u \in \mathbf{F}_q} \chi(u - 1) = 0.$$

Thus,  $S(\chi, x_{II}) = -\chi(4)J(\chi)$ . Observing that  $\Delta_{x_{II}} = 4r^3$  and that  $\lambda(x_{II}) = -1$ , this establishes Theorem 1 for all  $x$   $G$ -equivalent to  $x_{II}$ .

To treat the third case we introduce

$$x'_{III} = (s^2, 0, 0, -1) \quad \text{and} \quad x''_{III} = (1, 0, 0, -1).$$

$x'_{III}$  is  $G$ -equivalent to  $x_{III}$  (because its splitting field is also  $\mathbf{F}_{q^3}$ ), and  $x''_{III}$  is  $G$ -equivalent to  $x_I$ . Thus, by (1.1), (1.2), and (2.2),

$$S(\chi; x'_{III}) = \chi(s^2)S(\chi; x_{III}) + 1 - \chi(s^2),$$

and

$$S(\chi; x''_{III}) = S(\chi; x_I) - 1 = J(\chi) - 1.$$

Once again, a partitioning argument shows that

$$S(\chi; x_{III}) + S(\chi; x'_{III}) + S(\chi; x''_{III}) = 3 \sum_{u \in \mathbf{F}_q} \chi(u - 1) = 0.$$

Thus,  $(1 + \chi(s^2))S(\chi; x_{III}) = \chi(s^2) - J(\chi)$ , and since  $1 + \chi(s) + \chi(s^2) = 0$ , this implies

$$S(\chi; x_{III}) = \chi(s^2)J(\chi) - \chi(s).$$

The proof of Theorem 1 is completed for  $q \equiv 1 \pmod 6$  by noting that  $\Delta_{x_{III}} = -27s^2$ .

When  $q$  is even, all the above arguments are valid except that pertaining to the orbit of forms whose splitting field is  $\mathbf{F}_{q^2}$ . For this case, consider the additive map  $\phi(u) = u^2 + u$ . The kernel is  $\mathbf{F}_2$ , and therefore the cardinality of  $\phi(\mathbf{F}_q)$  is  $q/2$ . For any  $\alpha \in \mathbf{F}_q$ , define  $x(\alpha) = (0, 1, 1, \alpha)$ . If  $\alpha \notin \phi(\mathbf{F}_q)$ , then the splitting field of  $F_{x(\alpha)}$  is  $\mathbf{F}_{q^2}$ . Since the characteristic is 2,  $\Delta_{x(\alpha)} = 1$  for all  $\alpha$ . Fix a particular  $\beta \notin \phi(\mathbf{F}_q)$ . Then

$$S(\chi; x(\alpha)) = \begin{cases} S(\chi; x(0)) = J(\chi), & \text{if } \alpha \in \phi(\mathbf{F}_q), \\ S(\chi; x(\beta)), & \text{if } \alpha \notin \phi(\mathbf{F}_q). \end{cases}$$

On the other hand,

$$\sum_{\alpha \in \mathbf{F}_q} S(\chi; x(\alpha)) = \sum_{\alpha \in \mathbf{F}_q} \sum_{u \in \mathbf{F}_q} \chi(u^2 + u + \alpha) = \sum_{u \in \mathbf{F}_q} \sum_{\alpha \in \mathbf{F}_q} \chi(\alpha) = 0.$$

All these results together imply

$$S(\chi; x(\beta)) = -J(\chi).$$

This proves the last case left of Theorem 1. Q.E.D.

PROOF OF THEOREM 2. First of all, singular forms make no contribution to the sum of Theorem 2 since  $\bar{\chi}(0) = 0$ . Then, in light of Theorem 1, the stated sum reduces to

$$(q - 1)J(\chi)\{\text{Card}(G \cdot x_I) - \text{Card}(G \cdot x_{II}) + \text{Card}(G \cdot x_{III})\}.$$

By Lemma 3, the orbits of  $x_I$ ,  $x_{II}$ , and  $x_{III}$  have cardinality one-sixth, one-half, and one-third, respectively, of the cardinality of  $G$ . The theorem is now immediate. Q.E.D.

That the sum of Theorem 2 comes down to an alternating sum that vanishes suggests that this is a reflection of the geometry of the hypersurface of singular binary cubic forms. However, the exact relation is presently unclear to the author.

#### REFERENCES

1. B. Datskovsky and D. J. Wright, *The adelic zeta function associated with the space of binary cubic forms, II: Local theory*, J. Reine Angew. Math. **367** (1986), 27–75.
2. H. Davenport and H. Hasse, *Die Nullstellen der Kongruenz Zetafunktion in gewissen zyklischen Fällen*, J. Reine Angew. Math. **172** (1935), 151–182.
3. D. Friedman, *Cubic character sums and congruences*, Ph.D. Thesis, Univ. of California, Berkeley, 1967.
4. K. Ireland and M. Rosen, *A classical introduction to modern number theory*, Springer, 1982.
5. J. Lagarias, *Evaluation of certain character sums*, Master's Thesis, Massachusetts Institute of Technology, 1972.
6. T. Shintani, *On Dirichlet series whose coefficients are class-numbers of integral binary cubic forms*, J. Math. Soc. Japan **24** (1972), 132–188.
7. D. J. Wright, *The adelic zeta function associated with the space of binary cubic forms, I: Global theory*, Math. Ann. **270** (1985), 503–534.

DEPARTMENT OF MATHEMATICS, OKLAHOMA STATE UNIVERSITY, STILLWATER, OKLAHOMA, 74078-0613

*Current address:* Sonderforschungsbereich 170, Mathematisches Institut, Bunsenstrasse 3–5, 3400 Göttingen, Federal Republic of Germany