Alaca, Şaban

Congruences for Brewer sums. (English) Zbl 1107.11032

Finite Fields Appl. 13, No. 1, 1-19 (2007).

The Brewer sums considered here are

$$\Lambda_n(a) = \sum_{x=0}^{p-1} L(D_n(x,a),p),$$

where p is a prime, L is the Legendre symbol and $D_n(x,a)$ is the nth order Dickson polynomial of the first kind. $\Lambda_n(a)$ is easily seen to be 0 when $(n, p^2-1) = 1$ or $p \equiv 3 \pmod 4$. The author considers the case where $p \equiv 1 \pmod 4$, n is an odd prime dividing p^2-1 and determines which $\Lambda_n(a)$ are 0. The proof uses explicit factorizations of the Dickson polynomials over finite fields.

Reviewer: Robert Fitzgerald (Carbondale)

MSC:

11L10 Jacobsthal and Brewer sums; other complete character sums
11T06 Polynomials over finite fields
12Y05 Computational aspects of field theory and polynomials (MSC2010)

Keywords:

Brewer sums; Dickson polynomials; finite fields

Full Text: DOI

References:

[1] Berndt, B.C.; Evans, R.J.; Williams, K.S., Gauss and Jacobi sums, (1998), Wiley New York · Zbl 0906.11001

[2] Bhargava, M.; Zieve, M.E., Factoring dickson polynomials over finite fields, Finite fields appl., 5, 103-111, (1999) · Zbl 0929.11060

[3] Brewer, B.W., On certain character sums, Trans. amer. math. soc., 99, 241-245, (1961) · Zbl 0103.03205

[4] Brewer, B.W., On primes of the form $u^2 + 5 v^2$, Proc. amer. math. soc., 17, 502-509, (1966) · Zbl 0147.29801

[5] Chou, W.-S., The factorization of dickson polynomials over finite fields, Finite fields appl., 3, 84-96, (1997) · Zbl 0910.11052

[6] Leprévost, F.; Morain, F., Revêtements de courbes elliptiques à multiplication complexe par des courbes hyperelliptiques et sommes de caractères, J. number theory, 64, 165-182, (1997) · Zbl 0874.11044

[7] R. Lidl, G.L. Mullen, G. Turnwald, Dickson Polynomials, Pitman Monograph, vol. 65, Longman Sci. Tech., Harlow, UK, 1993.

[8] Lidl, R.; Niederreiter, H., Finite fields, (1997), Cambridge University Press Cambridge

[9] Williams, K.S., Note on Dickson's permutation polynomials, Duke math. J., 38, 659-665, (1971) · Zbl 0235.12011