PACIFIC JOURNAL OF MATHEMATICS
Vol. 96, No. 1, 1981

ROUND TRINOMIALS

RICHARD W. MARSH, W. H. MILLS, ROBERT L. WARD
HOWARD RUMSEY, JR. AND LLOYD R. WELCH

Let $F(x)$ be a polynomial of degree D. We say that $F(x)$ is *round* if all its irreducible factors have relatively small degree (e.g., bounded by a small multiple of $\log D$). In the present paper we introduce new methods for the study of round polynomials. Using these methods we prove the existence of many classes of round trinomials over $GF(2)$, including all the previously known ones as well as many new ones.

Let $F(x)$ be a polynomial over $GF(2)$, and let α be a root of $F(x)$. Let Q be a power of 2, say $Q = 2^q$, and let σ be the automorphism of the splitting field of $F(x)$ defined by $\sigma\xi = \xi^Q$. We seek a linear relation over $GF(2)$ among $\alpha, \sigma\alpha, \sigma^2\alpha, \cdots, \sigma^m\alpha$ with m reasonably small. In § 2 we will show how to use such a linear relation to show that $F(x)$ is round.

The archetypical example of a round polynomial over $GF(2)$ is $F(x) = x^Q + x$. The irreducible factors of $F(x)$ are precisely all the irreducible polynomials whose degrees are divisors of q. Here we have $\sigma\alpha + \alpha = 0$, which is a linear relation of the desired type. The methods of § 2 show that this linear relation implies that the degree of the irreducible factor of $F(x)$ satisfied by α must divide q.

Our example is extended below to other cases in which the exponents of $F(x)$ are expressed in terms of Q. Even more generally we will consider polynomials $F(x)$ over $GF(2)$ whose exponents depend on two powers of 2, Q and R, and where the linear relation among the $\sigma^i\alpha$ has coefficients in $GF(R)$.

Our methods can clearly be generalized to work on polynomials over arbitrary finite fields—generalizations to polynomials over other finite fields of characteristic 2 are particularly easy, but we are primarily interested in trinomials over $GF(2)$, so we will stick to this case. Some of the old results we present have already been generalized to arbitrary finite fields and we will content ourselves with giving appropriate references.

Most of the results of this paper were first suggested by actual factorizations of trinomials, and then later proofs were found. Indeed a table of all trinomial factorizations over $GF(2)$ through degree 599 was compiled by the authors using a CDC-6600 computer program written by Neal Zierler. All of the really striking examples of round trinomials that were found this way can be accounted for by the theorems of this paper.