over GF(p) are known. More generally, in this paper the authors give a primitive polynomial of the third kind of degree n over GF(p^d) for each p, d, n satisfying $p < 10^2$, $p^d < 10^3, p^{dn} < 10^6$. Each GF($p^d$) is the exponential representation of [1, Section 3] as defined by the polynomial given here of degree d over GF(p). Under the natural lexicographic order on GF$[p^d, x]$, each of these polynomials is the first primitive polynomial of the third kind of its degree over GF(p^d). They were obtained through a search option in a software package developed by the authors and based on techniques described in [1]. Exhaustive tables of prime polynomials and the three kinds of primitive polynomials have been compiled for the smaller cases and degrees, portions of which will appear in due time. Those given in this paper are to be found on a microfiche card at the back of this journal.

The authors are indebted to the staff of the University Computer Center for their continuing cooperation and assistance. Particular thanks are extended to the Director, Melvin L. Pierce, and to Thomas R. Kennedy.

Department of Mathematics
The University of Texas at Arlington
Arlington, Texas 76019

1. J. T. B. BEARD, JR., "Computing in GF(q)," *Math. Comp.*, v. 28, 1974, pp. 1159–1166.

Factorization Tables for $x^n - 1$ Over GF(q)

By Jacob T. B. Beard, Jr.* and Karen I. West

Abstract. These tables give the complete factorization of $x^n - 1$ over GF(q), $q = p^a$, $2 \leqslant n \leqslant d$ as below, together with the Euler Φ-function of $x^n - 1$ whenever $\Phi(x^n - 1) < 10^8$.

$q = 2$; $d = 32$	$q = 3$; $d = 27$	$q = 11$; $d = 15$
$q = 2^2$; $d = 16$	$q = 3^2$; $d = 15$	$q = 13$; $d = 15$
$q = 2^3$; $d = 16$	$q = 5$; $d = 25$, $n \neq 23$†	$q = 17$; $d = 15$
$q = 2^4$; $d = 16$	$q = 5^2$; $d = 10$	$q = 19$; $d = 12$
$q = 2^5$; $d = 12$	$q = 7$; $d = 15$	$q = 23$; $d = 10$

This paper gives the complete factorization of $x^n - 1$ over GF(q), $q = p^a$, as indi-

Received October 11, 1973.

AMS (MOS) subject classifications (1970). Primary 12C05, 12C30. Secondary 12E05.

Key words and phrases. Factorization, Galois field, Euler Φ-function.

*This author was partially supported by an Organized Research Grant from the University of Texas at Arlington.

†*Added at galley by the authors.* $(x^{23} - 1)/(x - 1)$ is prime in GF$[5, x]$ by 33. Theorem in Dickson's *Linear Groups.*

cated in the abstract. These tables are to be found at the back of this journal on a microfiche card. In addition, the generalized Euler Φ-function is given whenever $\Phi(x^n - 1) < 10^8$. The representation used for $GF(p^a)$, $a > 1$, is discussed in [1, Section 3], while $GF(p)$ is represented as usual by the integers *modulo* p. Briefly, for $a > 1$ the additive identity of $GF(p^a)$ is denoted by Z, while $\alpha \in GF(p^a)^* = \{0, 1, \cdots, p^a - 2\}$ is an exponent for a cyclic generator for $GF(p)^*$. For appropriate table headings, the defining polynomial $F(x)$ of $GF(p^a)$ is given and remains the same as listed in [2]. Each table gives n, the prime factorization of $x^n - 1$, and $\Phi(x^n - 1) < 10^8$. All nonlinear polynomials are given in ascending order by degree, with the variable factor suppressed in each term. Linear factors are given in the form $x - \alpha$, displaying the root α. Hence the factorization

$$f(x) = (1 - a_1)(1 - a_2)(b_0 + b_1 + 1)(c_0 + c_1 + c_2 + 1)$$

represents the product

$$f(x) = (x - a_1)(x - a_2)(b_0 + b_1 x + x^2)(c_0 + c_1 x + c_2 x^2 + x^3).$$

Also, each factorization is naturally ordered according to the degrees of the factors.

The tables were obtained using a software package developed by the authors and run on a Xerox $\Sigma 7$. The importance of the factorization of $x^n - 1$ over $GF(q)$ is well known. In particular, this output enables the computation of all admissible q-polynomials (Ore, [3]) for elements of $GF(q^n)$, since each such monic q-polynomial

$$\sum_{i=0}^{m} a_i x^{q^i} \in GF[q, x^q]$$

corresponds to a divisor

$$\sum_{i=0}^{m} a_i x^i$$

of $x^d - 1$ over $GF(q)$ for some divisor d of n. This allows a significant improvement of the corresponding algorithm in [1, Section 4].

Department of Mathematics
The University of Texas at Arlington
Arlington, Texas 76019

1. J. T. B. BEARD, JR., "Computing in $GF(q)$," *Math. Comp.*, this issue.

2. J. T. B. BEARD, JR. & K. I. WEST, "Some primitive polynomials of the third kind," *Math. Comp.*, v. 28, 1974, pp. 1166–1167.

3. O. ORE, "Contributions to the theory of finite fields," *Trans. Amer. Math. Soc.*, v. 36, 1934, pp. 243–274.