MATHEMATICS OF COMPUTATION, VOLUME 30, NUMBER 133
JANUARY 1976, PAGES 179–183

# Factorization Tables for Trinomials Over GF$(q)$

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

**Abstract.** Tables placed in the UMT file give the complete factorization over GF$(q)$, $q = p^a$, of each trinomial $T(x)$ of degree $n$, $2 \leqslant n \leqslant d$, as below, together with the generalized Euler $\Phi$-function whenever $T(x)$ is not prime and $\Phi(T(x)) < 10^8$. In addition, the numerical exponent and $q$-polynomial is given for each $T(x)$ whenever $2 \leqslant n \leqslant d_1$.

| | |
|---|---|
| $q = 2$: $d = 20, d_1 = 18,$ | $q = 5$: $d = 15, d_1 = 8,$ |
| $q = 2^2$: $d = 16, d_1 = 10,$ | $q = 7$: $d = 10, d_1 = 7,$ |
| $q = 2^3$: $d = 9, d_1 = 7,$ | $q = 11$: $d = 7,$ |
| $q = 2^4$: $d = 8,$ | $q = 13$: $d = 7,$ |
| $q = 3$: $d = 18, d_1 = 9,$ | $q = 17$: $d = 7,$ |
| $q = 3^2$: $d = 9,$ | $q = 19$: $d = 7.$ |

On a microfiche card with this note, selected results from the above appear as Table I–Table IV as follows:

| | |
|---|---|
| $q = 2$: $d = 20, d_1 = 18,$ | $q = 3$: $d = 11, d_1 = 9,$ |
| $q = 2^2$: $d = 8, d_1 = 8,$ | $q = 5$: $d = 5, d_1 = 5.$ |

As evidenced by these tables, there does not necessarily exist a prime trinomial of given degree $n$ over arbitrary GF$(q)$.

**1. Introduction and Notation.** The tables, both those placed in the UMT file and Table I–Table IV to be found on a microfiche card at the back of this issue, give the complete factorizations of all trinomials $T(x)$ over GF$(q)$ as indicated in the abstract, where $T(x)$ is monic and $x \nmid T(x)$. The generalized Euler $\Phi$-function is given whenever $T(x)$ is not prime and $\Phi(T(x)) < 10^8$, and in some instances the numerical exponent and $q$-polynomial belonging to $T(x)$ are given. Although the $q$-polynomial belonging to $g(x)$ (Ore [7]) is well defined for arbitrary $g(x) \in \mathrm{GF}[q, x]$, "the numerical exponent" of nonprime $g(x) \in \mathrm{GF}[q, x]$ is root dependent. The reader is cautioned that "the numerical exponent" assigned to a nonprime polynomial $T(x)$ in these tables is the multiplicative order of the companion matrix of $T(x)$. The tables complement those of Zierler and Brillhart [8] and were obtained on a Xerox $\Sigma 7$ using a software package developed by the authors. Readers interested in efficient algorithms for factoring in $\mathrm{GF}[q, x]$ should see [5] and [6].

Our terminology is that of [1]. Briefly, for monic polynomials $f(x) \in \mathrm{GF}[q, x]$, the Euler $\Phi$-function gives the number $\Phi(f(x))$ of monic polynomials $g(x) \in \mathrm{GF}[q, x]$

Received August 23, 1974; revised March 25, 1975.

*AMS (MOS) subject classifications* (1970). Primary 12C05, 12E05, 12E10; Secondary 12C30.

*Key words and phrases.* Factorization, Galois field, trinomial, Euler $\Phi$-function, numerical exponent, $q$-polynomial.

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

of degree $<\deg f(x)$ such that $(g(x), f(x)) = 1$. A prime (monic irreducible) polynomial $f(x) \in GF[q, x]$ of degree $m$ is called primitive of the first, second, or third kind as any root of $f(x)$ in $GF(q^m)$ respectively belongs to the numerical exponent $q^m - 1$, the $q$-polynomial $x^{q^m} - x$, or both.

2. **Description.** Our representation for $GF(p^a)$, $a > 1$, is discussed in [1], while $GF(p)$ is represented as usual by the integers *modulo p.* For $a > 1$, the additive identity of $GF(p^a)$ is denoted by $Z$, and each $\alpha \in GF(p^a)^* = \{0, 1, \ldots, p^a - 2\}$ is an exponent of a cyclic generator for $GF(p^a)^*$. The defining polynomial $F(x)$ of $GF(p^a)$, $a > 1$, is given in each appropriate table heading and remains the same as in [2]–[4]. Whenever numerical exponents and $q$-polynomials are given, each prime polynomial in the table is flagged by the conventions

#: prime but not primitive of the first or second kind;
*: primitive of the first kind but not primitive of the second kind;
**: primitive of the second kind but not primitive of the first kind;
***: primitive of the third kind, i.e., both first and second kind.

Each polynomial is written with the variable factor of each term suppressed and in increasing order by degree whenever nonlinear. Linear factors are given in the form $x - \alpha$, displaying the root. Hence, the factorization

$$T(x) = (x - a_0)(b_0 + b_1 x + x^2)(c_0 + c_1 x + c_2 x^2 + x^3)$$

is denoted by

$$T(x) = (1 - a_0)(b_0 + b_1 + 1)(c_0 + c_1 + c_2 + 1).$$

The $q$-polynomial

$$g(x) = d_0 + d_1 x^q + \ldots + d_{m-1} x^{q^{m-1}} + x^{q^m}$$

of $T(x)$ is then written

$$g(x) = d_0 + d_1 + \ldots + d_{m-1} + 1.$$

For $\deg T(x) = n$ and $T(x)$ belonging to $x^{q^n} - x$, this maximal $q$-polynomial is always omitted.

3. **Distribution of Primes and Primitives.** Table A is based on the "complete" set of tables as placed in the UMT file, and for each $q$, $n$ gives the number of prime trinomials and primitive trinomials of the first, second, or third kind of degree $n$ over $GF(q)$. An entry of "–" displays the number is not known. However, additional information is available in such a case: consider the subtable

| $q$ | $n$ | Pr | 1st | 2nd | 3rd |
|---|---|---|---|---|---|
| 3 | 12 | 4 | – | 0 | 0 |
| | 13 | 12 | – | – | – |

Whenever the number of primitive trinomials of the first kind is not given, the programs do not calculate *any* information toward deciding whether the trinomials of that degree or larger are primitive of *any* kind. We have "completed" the last two columns by inspection, using the fact observed earlier [1] that if $x^n + \alpha x^k + \beta$ is primitive of the second kind, then $k = n - 1$. Hence for $q = 3$, we conclude from the table that the sum of the roots of each prime trinomial of degree 12 is zero, but that there is at least one prime trinomial of degree 13 whose root sum is nonzero. For given $n$, $q$ we observe there does not necessarily exist a prime trinomial of degree $n$ over GF($q$), much less one which is primitive of the first kind. Since the companion matrix of a primitive trinomial is sparse, such primitives are of interest in various contexts [1], [5]. It is hoped that empirical use of these tables will lead to existence characterizations and related results.

### TABLE A

*Distribution of Primitive Trinomials*

| $q$ | $n$ | Pr | 1st | 2nd | 3rd | $n$ | Pr | 1st | 2nd | 3rd |
|---|---|---|---|---|---|---|---|---|---|---|
| 2 | 2 | 1 | 1 | 1 | 1 | 12 | 4 | 0 | 0 | 0 |
| | 3 | 2 | 2 | 1 | 1 | 13 | 0 | 0 | 0 | 0 |
| | 4 | 2 | 2 | 1 | 1 | 14 | 2 | 0 | 0 | 0 |
| | 5 | 2 | 2 | 0 | 0 | 15 | 6 | 6 | 1 | 1 |
| | 6 | 3 | 2 | 1 | 1 | 16 | 0 | 0 | 0 | 0 |
| | 7 | 4 | 4 | 1 | 1 | 17 | 6 | 6 | 0 | 0 |
| | 8 | 0 | 0 | 0 | 0 | 18 | 5 | 2 | 0 | 0 |
| | 9 | 4 | 2 | 1 | 0 | 19 | 0 | 0 | 0 | 0 |
| | 10 | 2 | 2 | 0 | 0 | 20 | 4 | 2† | 0 | 0 |
| | 11 | 2 | 2 | 0 | 0 | | | | | |
| $2^2$ | 2 | 6 | 4 | 6 | 4 | 10 | 6 | 0 | 0 | 0 |
| | 3 | 6 | 0 | 3 | 0 | 11 | 18 | – | – | – |
| | 4 | 0 | 0 | 0 | 0 | 12 | 0 | 0 | 0 | 0 |
| | 5 | 18 | 8 | 6 | 4 | 13 | 12 | – | 0 | 0 |
| | 6 | 4 | 0 | 0 | 0 | 14 | 0 | 0 | 0 | 0 |
| | 7 | 12 | 0 | 3 | 0 | 15 | 30 | – | – | – |
| | 8 | 0 | 0 | 0 | 0 | 16 | 0 | 0 | 0 | 0 |
| | 9 | 12 | 0 | 3 | 0 | | | | | |
| $2^3$ | 2 | 28 | 18 | 28 | 18 | 6 | 63 | 36 | 21 | 18 |
| | 3 | 42 | 36 | 21 | 18 | 7 | 28 | 0 | 7 | 0 |
| | 4 | 56 | 36 | 28 | 18 | 8 | 0 | 0 | 0 | 0 |
| | 5 | 14 | 0 | 0 | 0 | 9 | 84 | 0 | 0 | 0 |

† Determined by Zierler and Brillhart [8].

Table A (*continued*)

| $q$ | $n$ | Pr | 1st | 2nd | 3rd | $n$ | Pr | 1st | 2nd | 3rd |
|---|---|---|---|---|---|---|---|---|---|---|
| $2^4$ | 2 | 120 | – | – | – | 6 | 80 | – | 0 | 0 |
| | 3 | 150 | – | – | – | 7 | 300 | – | – | – |
| | 4 | 0 | 0 | 0 | 0 | 8 | 0 | 0 | 0 | 0 |
| | 5 | 210 | – | – | – | | | | | |
| 3 | 2 | 2 | 2 | 2 | 2 | 11 | 8 | – | 0 | 0 |
| | 3 | 4 | 2 | 2 | 1 | 12 | 4 | – | 0 | 0 |
| | 4 | 7 | 5 | 2 | 2 | 13 | 12 | – | – | – |
| | 5 | 8 | 6 | 2 | 1 | 14 | 6 | – | – | – |
| | 6 | 12 | 8 | 0 | 0 | 15 | 8 | – | 0 | 0 |
| | 7 | 12 | 10 | 0 | 0 | 16 | 14 | – | 0 | 0 |
| | 8 | 17 | 11 | 0 | 0 | 17 | 4 | – | – | – |
| | 9 | 4 | 2 | 0 | 0 | 18 | 6 | – | 0 | 0 |
| | 10 | 2 | – | 0 | 0 | | | | | |
| $3^2$ | 2 | 32 | – | – | – | 6 | 24 | – | 0 | 0 |
| | 3 | 48 | – | – | – | 7 | 80 | – | – | – |
| | 4 | 48 | – | – | – | 8 | 48 | – | 0 | 0 |
| | 5 | 80 | – | – | – | 9 | 48 | – | 0 | 0 |
| 5 | 2 | 8 | 4 | 8 | 4 | 9 | 8 | – | 0 | 0 |
| | 3 | 16 | 8 | 8 | 4 | 10 | 8 | – | 0 | 0 |
| | 4 | 12 | 0 | 0 | 0 | 11 | 40 | – | – | – |
| | 5 | 16 | 8 | 4 | 2 | 12 | 36 | – | – | – |
| | 6 | 24 | 8 | 4 | 4 | 13 | 8 | – | 0 | 0 |
| | 7 | 24 | 24 | 8 | 8 | 14 | 12 | – | 0 | 0 |
| | 8 | 4 | 4 | 0 | 0 | 15 | 16 | – | 0 | 0 |
| 7 | 2 | 18 | 8 | 18 | 8 | 7 | 36 | 12 | 6 | 2 |
| | 3 | 24 | 6 | 12 | 3 | 8 | 48 | – | – | – |
| | 4 | 36 | 0 | 12 | 0 | 9 | 48 | – | – | – |
| | 5 | 36 | 12 | 12 | 4 | 10 | 30 | – | – | – |
| | 6 | 24 | 0 | 0 | 0 | | | | | |
| 11 | 2 | 50 | – | – | – | 5 | 60 | – | – | – |
| | 3 | 80 | – | – | – | 6 | 120 | – | – | – |
| | 4 | 90 | – | – | – | 7 | 120 | – | – | – |
| 13 | 2 | 72 | – | – | – | 5 | 120 | – | – | – |
| | 3 | 96 | – | – | – | 6 | 144 | – | – | – |
| | 4 | 108 | – | – | – | 7 | 144 | – | – | – |

TABLE A (*continued*)

| $q$ | $n$ | Pr | 1st | 2nd | 3rd | $n$ | Pr | 1st | 2nd | 3rd |
|---|---|---|---|---|---|---|---|---|---|---|
| 17 | 2 | 128 | – | – | – | 5 | 224 | – | – | – |
| | 3 | 192 | – | – | – | 6 | 320 | – | – | – |
| | 4 | 192 | – | – | – | 7 | 224 | – | – | – |
| 19 | 2 | 162 | – | – | – | 5 | 288 | – | – | – |
| | 3 | 216 | – | – | – | 6 | 324 | – | – | – |
| | 4 | 270 | – | – | – | 7 | 324 | – | – | – |

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

Mobil Research & Development Corporation
Dallas, Texas 75211

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

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. J. T. B. BEARD, JR. & K. I. WEST, "Factorization tables for $x^n - 1$ over GF($q$)," *Math. Comp.*, v. 28, 1974, pp. 1167–1168.

4. J. T. B. BEARD, JR. & K. I. WEST, "Factorization tables for binomials over GF($q$)," *Math. Comp.* (Submitted.)

5. E. R. BERLEKAMP, *Algebraic Coding Theory*, McGraw-Hill, New York, 1968. MR 38 #6873.

6. R. J. McELIECE, "Factorization of polynomials over finite fields," *Math. Comp.*, v. 23, 1969, pp. 861–867. MR 41 #1694a.

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

8. N. ZIERLER & J. BRILLHART, "On primitive trinomials (Mod 2)," *Information and Control*, v. 13, 1968, pp. 541–554. MR 38 #5750.