MATHEMATICS OF COMPUTATION, VOLUME 28, NUMBER 128
OCTOBER 1974, PAGES 1159–1168

Computing in GF(q)

By Jacob T. B. Beard, Jr. *

Abstract. This paper gives an elementary deterministic algorithm for completely factoring any polynomial over GF(q), $q = p^d$, criteria for the identification of three types of primitive polynomials, an exponential representation for GF(q) which permits direct rational calculations in GF(q) as opposed to modular arithmetic over GF[p, x], and a matrix representation for $\overline{\mathrm{GF}}(p)$ which admits computer computations. The third type of primitive polynomial examined permits the given representation of GF(q) to display a primitive normal basis over GF(p). The techniques developed require only the usual addition and multiplication of square matrices over GF(p). Partial tables from computer programs based on certain of these results will appear in later papers.

1. Introduction and Notation. Let F be an arbitrary field and let $(F)_n$ denote the algebra of all $n \times n$ matrices over F under the usual matrix addition and multiplication. If $g(x) \in F[x]$ is monic of degree n, we let $C(g(x)) \in (F)_n$ denote the companion matrix of $g(x)$. The set of all scalar matrices αI_n of order n, $\alpha \in F$, is denoted $S_n(F)$. From [2, Theorem 4] the ring extension $S_n(F)[C(g(x))]$ of $S_n(F)$ by the matrix $C(g(x))$ has no nonzero divisors of zero if $g(x)$ is prime in $F[x]$. The converse is seen on remembering

$$S_n(F)[C(g(x))] = \{h(C(g(x))) : h(x) \in F[x], \deg h(x) < n\} \tag{1.1}$$

and that $g(x)$ is the minimal polynomial of $C(g(x))$ over F. This irreducibility criterion is the foundation for the basic algorithm we develop in Section 2. This algorithm and its present variations rely only on semi-intelligent brute force, yet it exhibits the utility of the representation for GF(q) as given in Section 3. It is that representation for GF(q) which we stress at this time and which we anticipate may permit advances in general computer techniques involving Galois fields, especially concerning previously known and more sophisticated factorization routines [3], [4]. A usual sieve

Received May 14, 1973.

AMS (MOS) subject classifications (1970). Primary 12–04, 12C05, 12C15, 12F10.

Key words and phrases. Factorization, arithmetic in finite fields, irreducibility criterion, primitive polynomials, primitive normal bases, Euler function, exponent, linear polynomial, algebraic closure.

*This research was partially supported by the University of Texas Graduate Development Program and Organized Research Grants.

for factoring in $GF[q, x]$ which uses the representation is operational, but it is hoped that further attention to the matrix algebras (1.1) themselves will lead to a truly elegant algorithm for factoring $g(x)$. The representation in Section 5 for an algebraic closure $GF(p)$ of $GF(p)$ is machine admissible and offers certain advantages. The identification of primitive polynomials in Section 4 was undertaken and included at the suggestion of L. Carlitz, to whom the author is most grateful. Partial computer results based on these techniques will appear in later papers, while extensive tables are prepared but unpublished. Reasonable requests for specific results are invited.

2. The Basic Algorithm. Let $F_p = GF(p)$ and let $q = p^d$. It suffices to factor monic polynomials $g(x) \in GF[q, x]$ having nonzero constant term and satisfying $\deg g(x) = n \geqslant 2$. By an earlier construction [2, Theorem 11], we represent $GF(q)$ as a field F of $d \times d$ matrices over F_p, $F = S_d(F_p)[C(f(x))]$, where $f(x) \in F_p[x]$ is any fixed prime polynomial of degree d. Let $C = C(g(x))$ be the companion matrix (in $(F_p)_{nd}$) of the natural polynomial $g(x) \in F[x]$ and consider the set

$$M = \{h(C) : h(x) \in F[x],\ 0 < \deg h(x) < n,\ h(x) \text{ monic},\ h(0) \neq 0\}, \tag{2.1}$$

noting that $M \subset S_n(F)[C] \subset (F_p)_{nd}$. Order the set M by any scheme such that the corresponding sequence of degrees of the polynomials $h(x)$ is nondecreasing. This ordering of M induces an ordering on the set H_M of these polynomials $h(x)$ and induces a lexicographic order on the Cartesian product $M \times M$. Let M^2 be the usual set product as computable in the ring $(F)_n$ and observe that $M \times M$ determines a subarray of the multiplication table for $S_n(F)[C]$. If the zero matrix 0_{dn} is not contained in M^2, then $g(x)$ is prime and we are done. Otherwise, there exists a first element (A_i, A_j) in $M \times M$ such that $A_iA_j = 0_{dn} \in M^2$. In this case $i \leqslant j$, $g(x) = h_i(x)h_j(x)$, $h_i(x)$ is a prime factor of $g(x)$ of minimum degree, and $h_i(x)$ is the minimum prime factor of $g(x)$ in H_M. Hence $h_j(x)$ is prime in $F[x]$ if $\deg h_j(x) < 2 \deg h_i(x)$, and we are done. If $\deg h_j(x) \geqslant 2 \deg h_i(x)$, then $h_i(x)$ is the minimum *candidate* prime factor of $h_j(x)$ in H_M, in which case we redefine M (2.1) by setting $g(x) = h_j(x)$, $n = \deg h_j(x)$, and consider only those $h_k(C(h_j(x)))$ where $k \geqslant i$, retaining the original order on H_M. The complete factorization of our initial polynomial $g(x)$ is clearly obtained after at most $n - 1$ applications of this procedure.

Our basic algorithm constitutes a partial row search of the array of matrix products determined by $M \times M$ for each successive M (as necessary). We compute the matrices in the array in order, aborting any computation on obtaining a nonzero entry, and consider only those matrix products such that the degrees and constant terms of $g(x)$, $h_i(x)$, and $h_j(x)$ are consistent. In actual practice we modify the basic algorithm as follows. It is well known that for each matrix $h(C(g(x))) \in S_n(F)[C(g(x))]$ given by (1.1) this polynomial representation is unique, and that the first row vector of

$h(C(g(x)))$ displays the coefficients (in ascending order) of $h(x)$. Applying this knowledge to the array $M \times M$ with M as in (2.1), the algorithm holds on computing only the first row vectors of these matrix products and comparing them against the appropriate zero vector. We are reminded that in this instance, these are row vectors over $(F_p)_d$. This situation is improved in Section 3. The inefficiency of the trial and error search remains, unfortunately, so that the magnitude of the calculations involved makes even a usual sieve routine much more practical, given a "decent" representation for GF(q).

3. Representing GF(q). The algorithms presented in Section 2 are independent of the representation used for GF(q), and while all calculations were performed *modulo* p for $q = p^d$, there resulted a corresponding and considerable expenditure of time and available storage. We also seek an improvement over the usual methods of performing computations in GF(q) when $q \neq p$ [4] and represent GF(q) as follows. Using a modified sieve routine, we find a prime polynomial $g(x) \in F_p[x]$ of degree d. Checking initial row vectors, we choose $g(x)$ such that $C = C(g(x))$ has multiplicative order $q - 1$, so that the matrix C is a cyclic generator of the multiplicative group $S_n(F_p)[C]^* \cong$ GF(q)*, the isomorphism already established in [2, Theorem 2]. We associate the matrix $C^i \in S_n(F_p)[C]^*$ with the exponent i of C, $0 \leqslant i \leqslant q - 2$, and represent the set GF(q)* by

$$F^* = \{0, 1, \cdots, q - 2\}. \tag{3.1}$$

We choose to represent the set F externally by

$$F = \{Z, 0, 1, \cdots, q - 2\}, \tag{3.2}$$

and convert the character Z to -1 for our internal machine representation. This device proves useful whenever incrementation is performed. (It and many other practical suggestions are due to Karen I. West, the coauthor of several computer programs based on this paper.) It is clear that multiplication $\odot$ is defined on F^* by

$$r \odot s = r + s \pmod{q - 1} \tag{3.3}$$

and that the multiplicative inverse r^{-1} of $r \in F^*$ is given by

$$r^{-1} = q - r - 1. \tag{3.4}$$

Any kth roots of r are readily found by solving the linear congruence $kx \equiv r \pmod{q - 1}$, so that rational roots are easily calculated. Likewise, logarithms are trivial. From the identity $C^\alpha + C^\beta = C^\gamma(C^{\alpha-\gamma} + C^{\beta-\gamma})$, it is seen that addition $\oplus$ is completely defined on F^* by any one row of the addition table for the set F^*. In particular, we compute the entries of its first row

$$0 \oplus 0, 0 \oplus 1, \cdots, 0 \oplus (q - 2) \tag{3.5}$$

using the first row vectors of the matrices C^i, $0 \leqslant i \leqslant q - 2$, and denote these entries

from left to right as

$$\overline{0}, \overline{1}, \cdots, \overline{q-2} \tag{3.6}$$

to obtain

$$r \oplus s = \begin{cases} Z, \overline{r - s(\mathrm{mod}\ q-1)} = Z, \\ \overline{(r - s(\mathrm{mod}\ q-1) + s)(\mathrm{mod}\ q-1)}, \text{ otherwise}, \end{cases} \quad r, s \in F^*. \tag{3.7}$$

The additive inverse $\ominus r$ of $r \in F^*$ is given by

$$\ominus r = \begin{cases} r - j + q - 1, & r < j, \\ r - j, & r \geqslant j, \end{cases} \quad \text{where } \overline{j} = 0 \oplus j = Z. \tag{3.8}$$

Both (3.7) and (3.8) are seen on recognizing that the aforementioned identity causes any diagonal parallel to the principal diagonal of the *addition* table for F^* to exhibit *only* the entry Z, or else its entries occur in a natural "increasing order" *modulo* $q-1$ and no Z appears. Hence, our additive calculations in GF(p^d) with $d > 1$ are merely "diagonal" shifts. Since GF(p^m) is a subfield of GF(p^d) if and only if $m \mid d$, GF(p^m)* is generated cyclicly by a power of C, and GF(p^d) contains precisely one such subfield GF(p^m), then F readily displays its proper subfields. The fact that we continue to represent GF(p) by Z_p, the integers *modulo* p, is an inherent but nonfatal bug in our representation. Namely, that in extending GF(q) nontrivially, we must rename the elements of GF(q). A representation of GF(q) obtained by the techniques of Section 5 would not have this fault, and this is a primary advantage of working with $\overline{\mathrm{GF}(p)}$ as represented later. In Section 4, we examine a further condition on $g(x)$ so that our representation F for GF(q) displays a primitive normal basis over F_p. First, we remark on important details concerning the determination of the addition table for F^*.

To obtain the sums (3.5), the "brute force" approach is again highly impractical. No algebraic results known to the author yield a satisfactory partition of the array of initial row vectors of the matrices C^i such that the elements of F represented by their sums with the identity vector $[1, 0, \cdots, 0]$ are quickly identified. Indeed, (3.9) below indicates that no such partition exists. We avoid the (potential) comparison of these two arrays of row vectors as follows. Using the uniqueness of the initial row vectors of the C^i, we can apply the basis representation theorem from elementary number theory, base p. Let C^i have as its first row the vector $[\alpha_1 \cdots \alpha_d]$, and store i in $B(k)$ where $k = \Sigma_{j=0}^{d-1} \alpha_{j+1} p^j$. Then $\overline{i} = B(l)$ where $l = (\alpha_1 + 1)(\mathrm{mod}\ p) + \Sigma_{j=1}^{d-1} \alpha_{j+1} p^j$. Hence we have the sums (3.6) directly as

$$\overline{i} = \begin{cases} B(k+1), & \alpha_1 \neq p-1, \\ B(k-p+1), & \alpha_1 = p-1. \end{cases} \tag{3.9}$$

Given the appropriate defining polynomials $g(x) \in \mathrm{GF}[p, x]$ of degree d (see Section 4), Beard and West have obtained addition tables (3.5) for all $\mathrm{GF}(p^d)$ satisfying $p \leqslant 31$, $p^d < 33{,}000$ in 37.4 minutes (CPU) on an IBM 370/155. The time required for $\mathrm{GF}(2^{15})$ was 6.54 minutes (CPU).

4. Primitive Polynomials. Let $\alpha \in F = \mathrm{GF}(p^d)$ have minimal polynomial $f(x)$ over F_p. Historically, α is called a primitive element of F if and only if $p^d - 1$ is the smallest positive integer k such that $\alpha^k = 1$; i.e., if and only if α has order $p^d - 1$. Whenever k is this smallest positive integer the element α is said to belong to the numerical exponent k. If α is a primitive element of F, then $f(x)$ is called a primitive polynomial, and if α belongs to the numerical exponent k then $f(x)$ is said to belong to the numerical exponent k.

Ore introduced another type of primitive element as follows. Each $\beta \in F$ is a root of a unique monic polynomial $g(x) = \Sigma_{i=0}^{m} \alpha_i x^{p^i}$ in $F_p[x^p]$ of minimum degree $m \leqslant d$, and β is said to belong to the p-polynomial $g(x)$. If β belongs to $x^{p^d} - x$ Ore calls β a primitive element of F. This establishes another type of primitive polynomial—the minimal polynomial $h(x)$ of β over F_p where β belongs to $x^{p^d} - x$. Whenever $\beta \in F$ has minimal polynomial $h(x)$ over F_p and β belongs to $g(x) \in F_p[x^p]$, then $h(x)$ is said to belong to $g(x)$.

Carlitz [5] refers to α and β respectively as primitive elements of the first and second kind, and calls their corresponding minimal polynomials $f(x)$ and $g(x)$ *primitive polynomials of the first* and *second kind* respectively. We define $l(x) \in F_p[x]$ to be *primitive of the third kind* if and only if $l(x)$ is primitive of both the first and second kind. If $\beta \in \mathrm{GF}(p^d)$ is a primitive element of the second kind, then the set $\{\beta, \beta^p, \cdots, \beta^{p^{d-1}}\}$ is a normal basis for $\mathrm{GF}(p^d)$ over $\mathrm{GF}(p)$. If β is primitive of the first and second kind, i.e. *third kind*, Davenport [6] called $\{\beta, \beta^p, \cdots, \beta^{p^{d-1}}\}$ a primitive normal basis for $\mathrm{GF}(p^d)$ over $\mathrm{GF}(p)$ and showed that such a basis always exists. Carlitz [5] obtained the result earlier for p^d sufficiently large and considered a more general question. Given $k \mid p^d - 1$ and a p-polynomial $g(x) \mid x^{p^d} - x$, does there exist $\beta \in \mathrm{GF}(p^d)$ which belongs to both k and $g(x)$? The answer was affirmative for p^d large and k deg $g(x)$ sufficiently large. It is known to be negative in general, however, and our programs have contributed further information to appear in due time. Both Ore [7] and Carlitz [5] considered the generalized problem: if $\theta \in \mathrm{GF}(q^m)$, $q = p^d$, let $a(x) = \Sigma_{i=0}^{s} \alpha_i x^{q^i} \in \mathrm{GF}[q, x^q]$ be the unique monic q-polynomial of minimum degree $s \leqslant m$ such that $a(\theta) = 0$, and say that θ belongs to $a(x)$. If θ belongs to $x^{q^m} - x$ the set $\{\theta, \theta^q, \cdots, \theta^{q^{m-1}}\}$ is a normal basis for $\mathrm{GF}(q^m)$ over $\mathrm{GF}(q)$. Accordingly, we define a prime polynomial $f(x) \in \mathrm{GF}[q, x]$ of degree m to be *primitive of the first, second*, or *third kind* as any root θ of $f(x)$ in $\mathrm{GF}(q^m)$ respectively belongs to the numerical exponent $q^m - 1$, the q-polynomial $x^{q^m} - x$, or both. It is easily verified that all three of these concepts are root indepen-

dent since $f(x)$ is assumed prime. Ore [7] goes further and shows that any monic $g(x) \in \mathrm{GF}[q, x]$, prime or not, divides a unique monic q-polynomial $a(x) = \Sigma_{r=0}^{\gamma} \alpha_r x^{q^r} \in \mathrm{GF}[q, x^q]$ of minimum degree $\gamma \leqslant \deg g(x)$.

By Davenport's result [6], we can choose $g(x)$ in Section 3 to be primitive of the third kind so that the elements $1, p, \cdots, p^{d-1}$ of F^* (3.1) form a primitive normal basis for $\mathrm{GF}(p^d)$ over $\mathrm{GF}(p)$. More generally, we are able to find the q-polynomial to which any monic polynomial $g(x) \in \mathrm{GF}[q, x]$ belongs, $q = p^d$, $d \geqslant 1$. The technique follows immediately from observing that irregardless of the primality of $g(x)$, we have $g(x) | a(x)$ in $\mathrm{GF}[q, x]$ if and only if $a(C) = 0$, where $C = C(g(x))$, the companion matrix of $g(x)$. Again, we compute only the first row vector of $a(C)$. Observe that whenever the constant term of $g(x)$ is nonzero, the matrices C^{q^r} may be computed modulo the multiplicative order of C. A routine for finding the order of C is optimized by computing C^k for only the admissible values of k. These k are precisely the divisors of $\Phi(g(x))$, Φ the generalized Euler function on $\mathrm{GF}[q, x]$. This is seen since C is nonderogatory and has minimal polynomial $g(x)$ over $\mathrm{GF}[q, x]$, so that the order of the multiplicative group of nonsingular matrices in $S_m(\mathrm{GF}(q))[C]$ is $\Phi(g(x))$, where $m = \deg g(x)$.

Subject only to storage and time limitations, we are now able to factor any monic $f(x) \in \mathrm{GF}[q, x]$ satisfying $f(0) \neq 0$, find its q-polynomial, compute its numerical exponent whenever $f(x)$ is prime, and identify any prime $f(x)$ as being merely prime or primitive of the first, second, or third kind. For nonprime $f(x)$ we also calculate $\Phi(f(x))$. Our results are checked at run-time whenever possible against the following enumeration results, all trivially obtained from well-known results.

THEOREM 1. $\mathrm{GF}[q, x]$ *contains precisely* $\phi(q^m - 1)/m$ *primitive polynomials of the first kind of degree* m.

THEOREM 2. $\mathrm{GF}[q, x]$ *contains precisely* $\Phi(x^m - 1)/m$ *primitive polynomials of the second kind of degree* m.

Ore's observation [7] that $\mathrm{GF}(q^m)$ has precisely $\Phi(x^m - 1)/m$ distinct (unordered) normal bases over $\mathrm{GF}(q)$ leads directly to Theorem 2. The number N' of primitive elements of the third kind in $\mathrm{GF}(q^m)$ is known asymptotically in the general case due to Carlitz [5] and is given by

$$N' = \phi(q^m - 1)\Phi(x^m - 1)/q^m + O(q^{m(\frac{1}{2}+\epsilon)}).$$

THEOREM 3. $\mathrm{GF}[q, x]$ *contains precisely* N'/m *primitive polynomials of the third kind of degree* m.

Finally, the number of prime polynomials of given degree in $\mathrm{GF}[q, x]$ is checked against the result of Albert [1, p. 130]. One option of a program by Beard and West is a search for primitive polynomials of the third kind. At the present time a primitive polynomial of the third kind over $\mathrm{GF}(p^d)$ of degree n has been obtained for each p, d, n satisfying $p < 10^2, p^d < 10^3, p^{dn} < 10^6$. Under the natural lexi-

cographic order on $GF[p^d, x]$ as represented in Section 3, each of these polynomials is the first primitive polynomial of the third kind of its degree. The search for them was eased by the observation that the sum of the roots of $f(x)$ is nonzero whenever $f(x)$ is primitive of the second kind. Since our addition tables for $GF(q)$ are readily obtained (Section 3) once a primitive polynomial of the third (first) kind is known, we will publish this list of polynomials rather than the addition tables.

5. Representing $\overline{GF}(p)$. The remainder of this paper is devoted to obtaining a representation for an algebraic closure $\overline{GF}(p)$ of $GF(p)$. Let $(GF(p))_\infty$ denote the algebra of all row and column-finite matrices of infinite order over $GF(p)$. For $n \geqslant 1$ we will represent $GF(p^{n!})$ recursively as a subfield of $(GF(p))_\infty$. Berlekamp's [4] concept of $\overline{GF}(p)$ as $GF(p^{\infty!})$ is extremely nice, and we find it both appropriate and convenient to denote our representation of $\overline{GF}(p)$ by $GF(p^{\infty!})$. Not only are the operations in $GF(p^{\infty!})$ those of normal matrix addition and multiplication *modulo* p, but each matrix $A \in GF(p^{\infty!})$ exibits the smallest n such that $A \in GF(p^{n!})$. The construction of $GF(p^{\infty!})$ given here generalizes the extension technique developed in [2, Theorem 9] and our notation and terminology is that of [2] with only obvious modifications. Specifically we remember that for any square matrix A, the matrix k-sum(A) is the k-fold direct sum k-sum$(A) = \operatorname{diag}(A, \cdots, A)$, and that for any set T of square matrices we define k-sum$(T) = \{k\text{-sum}(A) : A \in T\}$.

For each m, $1 \leqslant m \leqslant \infty$, let I_m denote the multiplicative identity of the algebra $(GF(p))_m$, and let $S_m(GF(p))$ denote the field of all scalar matrices αI_m, $\alpha \in GF(p)$. Let $f_2(x)$ be any prime polynomial of degree 2 over $GF(p)$ and define

$$F_{2!} = S_2(GF(p))[C(f_2(x))],$$

so that $F_{2!} \cong GF(p^2)$ [2, Theorem 2]. We define $GF(p^{1!}) = S_\infty(GF(p))$ and $GF(p^{2!}) = \infty\text{-sum}(F_{2!})$, and have $GF(p^{1!}) \subset GF(p^{2!})$.

Let $f_3(x)$ be any prime polynomial of degree 3 over $F_{2!}$ and note that $GF(p^{2!}) = S_\infty(F_{2!})$. Using the companion matrix $C(f_3(x))$ in $(F_{2!})_3$ of $f_3(x)$, we define

$$F_{3!} = S_3(F_{2!})[C(f_3(x))].$$

Then $F_{3!} \cong GF(p^6)$ [2, Theorem 4] and we define

$$GF(p^{3!}) = \infty\text{-sum}(F_{3!}) = S_\infty(F_{3!})$$

so that $GF(p^{1!}) \subset GF(p^{2!}) \subset GF(p^{3!})$.

Having constructed $GF(p^{n!}) = S_n(F_{n!})$, we choose any prime polynomial $f_{n+1}(x)$ of degree $n+1$ over $F_{n!}$ and define

$$GF(p^{(n+1)!}) = S_\infty(F_{(n+1)!}),$$

where

$$F_{(n+1)!} = S_{n+1}(F_{n!})[C(f_{n+1}(x))]$$

and $C(f_{n+1}(x))$ in $(F_{n!})_{n+1}$ is the companion matrix of $f_{n+1}(x)$. Remembering the natural isomorphism between $(K_{n!})_{n+1}$ and $(K)_{(n+1)!}$ for arbitrary fields K, we see that $\mathrm{GF}(p^{(n+1)!})$ is a subfield of $(\mathrm{GF}(p))_\infty$ and has order $p^{(n+1)!}$. Furthermore, $\mathrm{GF}(p^{1!}) \subset \cdots \subset \mathrm{GF}(p^{n!}) \subset \mathrm{GF}(p^{(n+1)!})$. We define $\mathrm{GF}(p^{\infty!}) = \bigcup_{n=1}^{\infty} \mathrm{GF}(p^{n!})$ and are done.

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

1. A. A. ALBERT, *Fundamental Concepts of Higher Algebra*, Univ. of Chicago Press, Chicago, Ill., 1958. MR 20 #5190.

2. J. T. B. BEARD, JR., "Matrix fields over prime fields," *Duke Math. J.*, v. 39, 1972, pp. 313–322.

3. E. R. BERKLEKAMP, "Factoring polynomials over large finite fields," *Math. Comp.*, v. 24, 1970, pp. 713–735. MR 34 #1948.

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

5. L. CARLITZ, "Primitive roots in a finite field," *Trans. Amer. Math. Soc.*, v. 73, 1952, pp. 373–382. MR 14, 539.

6. H. DAVENPORT, "Bases for finite fields," *J. London Math. Soc.*, v. 43, 1968, pp. 21–39; ibid., v. 44, 1969, p. 378. MR 37 #2729; 38 #2127.

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

Some Primitive Polynomials of the Third Kind

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

Abstract. This paper gives the first primitive polynomial of the third kind of degree n over $\mathrm{GF}(p^d)$ for each p, d, n satisfying $p < 10^2, p^d < 10^3, p^{dn} < 10^6$.

In the preceding paper [1, Section 3] Beard introduced an exponential representation for $\mathrm{GF}(p^d)$ which allows full use of its multiplicative structure and permits direct rational calculations in $\mathrm{GF}(p^d)$. As indicated in [1, Section 4], such representations are easily and quickly obtained once primitive polynomials of the third kind of degree d

Received May 14, 1973.

AMS (MOS) subject classifications (1970). Primary 12–04, 12C05, 12C15.

Key words and phrases. Arithmetic in finite fields, primitive polynomials.

*This author was partially supported by the University of Texas Graduate Development Program and Organized Research Grants.