Factorization of Polynomials over Finite Fields

By Robert J. McEliece*

Abstract. If $f(x)$ is a polynomial over $GF(q)$, we observe (as has Berlekamp) that if $h(x)^q \equiv h(x) \pmod{f(x)}$, then $f(x) = \prod_{a \in GF(q)} \gcd(f(x), h(x) - a)$. The object of this paper is to give an explicit construction of enough such h's so that the repeated application of this result will succeed in separating all irreducible factors of f. The h's chosen are loosely defined by $h_i(x) \equiv x^i + x^{iq} + x^{iq^2} + \cdots \pmod{f(x)}$. A detailed example over $GF(2)$ is given, and a table of the factors of the cyclotomic polynomials $\Phi_n(x) \pmod{p}$ for $p = 2$, $n \leqq 250$; $p = 3$, $n \leqq 100$; $p = 5, 7$, $n \leqq 50$, is included.

I. Introduction. The object of this paper is to present a workable algorithm for factoring polynomials over finite fields. The existence of such an algorithm is not in doubt since it is clearly possible to generate recursively all irreducible polynomials of a given degree over a given finite field, and then test any polynomial for divisibility by the irreducibles, one by one; naturally such an algorithm is highly impractical for even low degrees. It is of course frequently necessary to be able to factor polynomials over finite fields; for example in factoring rational primes in algebraic number fields. The algorithm to be given is quite usable; for example over $GF(2)$ it is effective for hand calculations up to degree 15 or so, and with the aid of a computer it is possible to go up to degree several hundred without difficulty. Through the use of this algorithm we have constructed a table, appearing in the microfiche section of this issue, of the factors of $x^n - 1$ over $GF(p)$ for $p = 2$, $n \leqq 250$; $p = 3$, $n \leqq 100$; $p = 5$, $n \leqq 50$, $p = 7$, $n \leqq 50$. This table gives the factorization of the primes 2, 3, 5, 7 in the corresponding cyclotomic fields, and is also of use in studying linear recurrence relations of period n over $GF(p)$, since the characteristic polynomials of such recurrences are precisely the divisors of $x^n - 1$. Published tables of irreducible polynomials over finite fields are insufficient to factor $x^n - 1$ for even modest values of n; for example Marsh's table [1] of polynomials irreducible over $GF(2)$ up to degree 19 cannot be used to factor $x^{43} - 1$ over $GF(2)$.

Let us finally mention that Berlekamp [2] has recently published a similar algorithm, which shares Theorem 1, below, with ours, but proceeds in a somewhat different direction. A brief comparison of the two algorithms is given at the end of the next section.

II. The Algorithm. Throughout, let $F = GF(q)$, $q = p^r$, p a prime. If $f(x)$ and $g(x)$ are polynomials over F, denote by (f, g) their greatest common divisor, which we assume is monic. (We also adopt the convention $(f, a) = 1$ for $a \in F$.) We are given a polynomial $f(x)$ of degree n over F, and are asked to write f as a product of irreducible factors. We are free to assume that $f(x)$ is squarefree, since unless f is a

Received February 19, 1968, revised October 3, 1968.

* This paper presents the results of one phase of research carried out at the Jet Propulsion Laboratory, California Institute of Technology, under Contract No. NAS 7-100, sponsored by the National Aeronautics and Space Administration.

pth power, $f/(f, f')$ will be a nontrivial squarefree divisor of f. And while the algorithm can be applied to an arbitrary polynomial, squarefree or not, to find the irreducible powers which divide it, any preliminary reduction in the degree of f which can be made will shorten the computations. Thus $f(x)$ is henceforth squarefree. We further assume $f(0) \neq 0$. Under these circumstances there will be a smallest integer e such that $f(x) | x^e - 1$ and $(e, p) = 1$. e is called the *period* of f.

Theorem 1 gives a way to factor f, under certain circumstances:

THEOREM 1. *If* $h(x)^q \equiv h(x) \pmod{f(x)}$, *then*

$$f(x) = \prod_{a \in F} (f(x), h(x) - a) .$$

Proof. Let θ be a root of f in a splitting field K. Then $h(\theta)^q = h(\theta)$ and so $h(\theta)$, being fixed by the Galois group of K/F, is an element of F. Thus every root of f is a root of exactly one of the polynomials $h(x) - a$, and Theorem 1 follows.

Theorem 1 need not give a nontrivial factorization of f; if $h(x) \equiv a (\bmod f(x))$ for some $a \in F$, Theorem 1 is of no use. However, if Theorem 1 does give a nontrivial factorization of f, we say that h is an *f-reducing* polynomial; naturally h is automatically f-reducing if $0 < \deg h < n = \deg f$. (It will soon develop that f-reducing polynomials always exist if f is reducible.) The object of the rest of this section is to indicate a method of constructing f-reducing polynomials. There are two possible ways the algorithm could work: first, we could find just one f-reducing polynomial, and then inductively proceed to find reducing polynomials for the resulting factors; or, we could produce so many f-reducing polynomials that they themselves would reduce all resulting factors of f. We shall below give two similar families of f-reducing polynomials, corresponding to these two possibilities.

If we discover the least integer N such that $x^{q^N} \equiv x (\bmod f(x))$, then $N = \text{l.c.m.}(n_1, n_2, \cdots, n_t)$, where $f(x) = f_1(x) f_2(x) \cdots f_t(x)$ is the factorization of f into irreducibles with $\deg f_k = n_k$. N is the degree of the splitting field for f. Now consider the algebra R_f over $GF(q)$ of polynomials $y = y(x) \pmod{f(x)}$, and define the map $T(y) = y + y^q + y^{q^2} + \cdots + y^{q^{N-1}}$. Next we say that f_k is a *regular divisor* of f if N/n_k is not divisible by p. Note that regular divisors always exist.

THEOREM 2. *T is a $GF(q)$-linear function on R_f whose rank is equal to the number of regular divisors of F.* Range $(T) \subseteq GF(q)$ *if and only if f is irreducible.*

Proof. By a generalization of the well-known Chinese Remainder Theorem [3, p. 63] R_f is isomorphic to the direct sum $R_{f_1} \oplus \cdots \oplus R_{f_t}$ under the map $y \rightarrow (y_1, y_2, \cdots, y_t)$ with $y \equiv y_k \pmod{f_k(x)}$. Since the f_k are irreducible, the R_{f_k} are fields. Let T_k be the *trace* on R_{f_k}; i.e., $T_k(y) = y + y^q + \cdots + y^{q^{n_k - 1}}$. Then for $y \in R_{f_k}$, $T(y) = m_k T_k(y)$ where $m_k = N/n_k$. Thus for $y \in R_f$, $T(y) = T(y_1, y_2, \cdots, y_t) = (m_1 T_1(y_1), \cdots, m_t T_t(y_t))$, and so if $m_k = 0$ (i.e., f_k is irregular) the kth coordinate of $T(y)$ will be identically zero, and otherwise the kth coordinate ranges freely over $GF(q)$. This shows that dim range (T) = number of regular divisors. To prove the last sentence of Theorem 1, notice that in the isomorphism $R_f \cong R_{f_1} \oplus \cdots \oplus R_{f_t}$, $GF(q)$ appears as the diagonal; i.e. t-tuples of the form $(a, a, \cdots, a)$, $a \in GF(q)$. Clearly if $t \geqq 2$, range (T) cannot be contained in $GF(q)$ since as we have seen the nonzero coordinates of range (T) vary independently from one another. This completes the proof of Theorem 2.

Now since $1, x, x^2, \cdots, x^{n-1}$ are a basis for R_f over $GF(q)$, the polynomials

$T_i(x) = T(x^i) = x^i + x^{iq} + \cdots + x^{iq^{N-1}}$ span range (T). Furthermore $T_i(x)^q \equiv T_i(x) \pmod{f(x)}$, so we arrive at the important

COROLLARY 1. *The polynomials $T_i(x)$, $1 \leqq i < n$, include f-reducing polynomials unless f is already irreducible.*

Although the polynomials T_i of Corollary 1 enable us to begin the factorization of f, they are not usually able to reduce all the resulting factors. What is not difficult to show is that the best the T_i's allow is the factorization $f = f_1 \cdots f_j \bar{f}_{j+1}$ where $f_1, f_2, \cdots, f_j$ are the regular divisors of f and $\bar{f}_{j+1}$ is the product of the irregular divisors. Of course what one does in practice is compute the first f-reducing T_i, and then compute new T_i for each of the resulting factors. However, it is possible to give another set of polynomials, $R_i(x)$, which are capable of separating all the irreducible factors of f at once.

Definition. For each i, $1 \leqq i < e$, let m_i be the least integer such that $x^i \equiv x^{iq^{m_i}} \pmod{f(x)}$. (It is easy to see that $m_i = \text{ord}_{e/(e,i)}(q)$, but it is not necessary to know e in order to compute the m_i.) We define

$$R_i(x) \equiv x^i + x^{iq} + \cdots + x^{iq^{m_i-1}} \pmod{f(x)}\,.$$

Then the R_i clearly satisfy $R^q \equiv R \pmod{f(x)}$, and so they are certainly candidates for f-reducing polynomials; indeed $T_i(x) \equiv c_iR_i(x) \pmod{f(x)}$ for $c_i = N/m_i$, so that the R_i are certainly no worse than the T_i. We now show that the R_i, $1 \leqq i < e$, are capable of distinguishing all the factors of f. Two easy lemmas are required. We shall see that it is enough to consider the special case $f(x) = x^e - 1$.

LEMMA 1. *Let $f(x) = x^e - 1$ for some e prime to p. If $h(x)^q \equiv h(x) \pmod{x^e - 1}$, then $h(x)$ is a $GF(q)$-linear combination of the polynomials $R_i(x)$.*

Proof. We first describe the R_i. According to the definition let m_i be the smallest integer such that $x^i \equiv x^{iq^{m_i}} \pmod{x^e - 1}$; i.e., $i \equiv iq^{m_i} \pmod{e}$. Hence $R_i = x^i + x^{iq} + \cdots + x^{iq^{m_i-1}}$, and the exponents which occur are precisely the residues mod e which are obtained from i by multiplying by various powers of q. For example with $q = 3$, $e = 13$, the orbits are (0), (1, 3, 9), (2, 6, 5), (4, 12, 10), (7, 8, 11) and so $R_1 = R_3 = R_9 = x + x^3 + x^9$; $R_2 = R_6 = R_5 = x^2 + x^5 + x^6$, etc. Now suppose $h(x)^q \equiv h(x) \pmod{x^e - 1}$; if we let $h(x) = \sum_{k=0}^{e-1} h_k x^k$, then $h(x)^q \equiv h(x^q) = \sum h_k x^{qk}$, with exponents reduced mod e, if necessary. Hence $h_k = h_{kq} = h_{kq^2} = \cdots$ for all k, so that $h(x) = \sum_{k \in K} h_k R_k(x)$, where the set K contains exactly one member from each equivalence class of residues modulo e given by $k_1 \sim k_2$ if and only if $k_1 \equiv k_2 q^t \pmod{e}$ for some $t \geqq 0$.

LEMMA 2. *If f is an irreducible divisor of $x^e - 1$, then there is a polynomial g with $(x^e - 1, fg) = f$ and $(fg)^q \equiv fg \pmod{x^e - 1}$.*

Proof. Since $(e, p) = 1$, $x^e - 1$ is squarefree, and so $(f, (x^e - 1)/f) = 1$. Hence there is a g such that $fg \equiv 1 \pmod{(x^e - 1)/f}$. This implies $(fg)^2 \equiv fg \pmod{x^e - 1}$ and so also $(fg)^q \equiv fg \pmod{x^e - 1}$. Finally from $(g, (x^e - 1)/f) = 1$ follows $(fg, x^e - 1) = f$.

THEOREM 3. *Let f_1 and f_2 be distinct irreducible divisors of $x^e - 1$. Then there is an integer i, $1 \leqq i < e$, and distinct elements $a, b \in F$ such that*

$$R_i(x) \equiv a \pmod{f_1}\,, \qquad R_i(x) \equiv b \pmod{f_2}\,.$$

Hence the factors f_1 and f_2 can be "separated" by the factorization given in Theorem 1, using R_i.

Proof. Suppose, on the contrary, that for each i there is an element $a_i \in F$ such that $R_i(x) \equiv a_i \pmod{f_1f_2}$. By Lemma 2 there exists $h(x)$ such that $(f_1h)^q \equiv f_1h \pmod{x^e - 1}$ and $(f_1h, x^e - 1) = f_1$. Lemma 1 then shows that $f_1h \equiv \sum b_iR_i(x)$ for suitable $b_i \in F$. Our assumption implies that $f_1h \equiv \sum b_iR_i \equiv \sum a_ib_i \equiv b \pmod{f_1f_2}$; this implies $f_1h \equiv b \pmod{f_1}$ so that $b = 0$. On the other hand $f_1h \equiv 0 \pmod{f_1f_2}$ is in conflict with $(f_1h, x^e - 1) = f_1$, and the proof is complete.

COROLLARY. *For any squarefree $f(x)$, the corresponding $R_i(x)$, $1 \leqq i < e =$ period (f), will separate all irreducible factors of f.*

Proof. Denote by $R_i^{(e)}(x)$ the R's associated with $x^e - 1$. Theorem 3 shows us that the $R_i^{(e)}(x)$ suffice to separate all factors of $x^e - 1$, so they certainly suffice to separate the factors of f. On the other hand $x^{iq^m} \equiv x^i \pmod{x^e - 1}$ certainly implies that $x^{iq^m} \equiv x^i \pmod{f(x)}$, so that $R_i^{(e)}(x) \equiv k_iR_i(x) \pmod{f(x)}$ for suitable $k_i \in F$; thus the R_i can separate all the factors of f. (In fact it is not hard to see that $k_i = 1$ for all i.)

The corollary to Theorem 3 shows that the R_i, $1 \leqq i < e$, will separate the factors of f. One might hope, however, that only the R_i, $1 \leqq i < n$, would be needed, but this is not always the case. For example over $GF(2)$, if $f(x) = f_1f_2f_3$ with $\deg f_1 = \deg f_2 = 4$, $\deg f_3 = 8$, then $R_1, \cdots, R_{11}$ cannot separate f_1 from f_2. Hence the disadvantage in using the R_i is that it is in general necessary to compute a large number of them in order to be sure they will separate all factors. However, in the important special case $f(x) = x^e - 1$, the R_i are ideally suited. (See Example 2, below.)

Comparison with Berlekamp's Algorithm. The central point of Berlekamp's algorithm is that the equation $h(x)^q - h(x) \equiv 0 \pmod{f(x)}$ may be regarded as a homogeneous system of n simultaneous linear equations in the coefficients of h. Thus Berlekamp finds f-reducing polynomials by finding the nullspace of a certain $n \times n$ matrix over $GF(q)$. This amounts to row-reducing an $n \times n$ matrix, which turns out to require on the order of n^3 coordinate operations over $GF(q)$, and the amount of calculation is not highly dependent upon the polynomial being factored.

On the other hand, the analysis of the algorithm of this paper is not so simple, for the amount of calculation required depends very heavily on the integer N which in turn is highly sensitive to the factorization of f. For example consider squarefree polynomials $f(x)$ of degree 12 over $GF(2)$; if $f(x)$ is the product of the three irreducibles of degree four, $N = 4$, while degrees 3, 4 and 5 give $N = 60$. The mean value for N among all squarefree polynomials of degree 12 which have no linear factor is 16.4, and it seems reasonable to conjecture that the mean value of N grows linearly with n. (But one can show that the largest possible value of N grows faster than $\exp(n^a)$ for all $a < \frac{1}{2}$.) Thus to compute $T_i(x)$, one needs N successive qth powers of x^i (modulo $f(x)$), which requires n^2N coordinate operations. And since in general several T_i must be computed before an f-reducing polynomial is found, this algorithm is no better than Berlekamp's. However, the process of computing successive qth powers modulo f is a less complex operation than row-reducing an $n \times n$ matrix, so that the present algorithm is, for example, easier to program.

III. Examples.

1. Let us apply the algorithm to the polynomial $f(x) = x^{17} + x^{14} + x^{13} + x^{12} + x^{11} + x^{10} + x^9 + x^8 + x^7 + x^5 + x^4 + x + 1$ over $GF(2)$. $f(0) = 1$ and f is not

a square. Now $f' = x^{16} + x^{12} + x^{10} + x^8 + x^6 + x^4 + 1$. We compute (f, f') by Euclid's algorithm, abbreviating a polynomial $\sum_{i=0}^{n} a_i x^i$ by the $(n + 1)$-tuple $(a_n a_{n-1} \cdots a_1 a_0)$:

```
1 0 0 1 1 1 1 1 1 1 1 0 1 1 0 0 1 1
1 0 0 0 1 0 1 0 1 0 1 0 1 0 0 0 1
-----------------------------------
      1 0 1 0 1 0 1 0 0 0 1 0 0 0 1
      1 0 0 0 1 0 1 0 1 0 1 0 1 0 0 0 1
      -----------------------------------
          1 0 0 0 0 0 1 0 0 0 1 0 1 0 1
          1 0 1 0 1 0 1 0 0 0 1 0 0 0 1
          -----------------------------
              1 0 1 0 0 0 0 0 0 0 1 0 0
              1 0 1 0 1 0 1 0 0 0 1 0 0 0 1
              -----------------------------
                      1 0 1 0 0 0 0 0 0 0 1
                      1 0 1 0 0 0 0 0 0 0 1
                      ---------------------
```

Hence $(f, f') = x^{10} + x^8 + 1$, and an easy division gives $f/(f, f') = x^7 + x^5 + x^4 + x + 1 = \bar{f}$, which we now know to be squarefree. We now compute the $T_i(x)$, and to do so it is convenient to have a list of even powers of x modulo $\bar{f}$:

$$\begin{array}{ll} x^0 & = 0\ 0\ 0\ 0\ 0\ 0\ 1 \\ x^2 & = 0\ 0\ 0\ 0\ 1\ 0\ 0 \\ x^4 & = 0\ 0\ 1\ 0\ 0\ 0\ 0 \\ x^6 & = 1\ 0\ 0\ 0\ 0\ 0\ 0 \\ x^8 & = 1\ 1\ 0\ 0\ 1\ 1\ 0 \\ x^{10} & = 1\ 0\ 0\ 1\ 1\ 0\ 1 \\ x^{12} & = 1\ 0\ 1\ 0\ 0\ 1\ 0 \end{array}$$

(Berlekamp observed that the operation of squaring a polynomial

$$\sum_{i=0}^{n-1} a_i x^i \bmod f(x)$$

is the same as multiplying the vector $a_0 a_1 \cdots a_{n-1}$ by the $n \times n$ matrix of even powers.) We compute T_1:

$$\begin{array}{ll} x & = 0\ 0\ 0\ 0\ 0\ 1\ 0 \\ x^2 & = 0\ 0\ 0\ 0\ 1\ 0\ 0 \\ x^4 & = 0\ 0\ 1\ 0\ 0\ 0\ 0 \\ x^8 & = 1\ 1\ 0\ 0\ 1\ 1\ 0 \\ x^{16} & = 0\ 0\ 0\ 1\ 0\ 1\ 1 \\ x^{32} & = 1\ 0\ 0\ 0\ 1\ 0\ 1 \\ x^{64} & = 1\ 0\ 0\ 0\ 0\ 1\ 1 \\ x^{128} & = 1\ 0\ 1\ 0\ 1\ 1\ 1 \\ x^{256} & = 0\ 1\ 0\ 0\ 0\ 0\ 1 \\ x^{512} & = 1\ 0\ 0\ 1\ 1\ 0\ 0 \\ \hline T_1(x) & = 1\ 0\ 0\ 0\ 1\ 1\ 1 \end{array}$$

$x^{2^{10}} = x$, hence $N = 10$.

$T_1(x)$ is therefore an $\bar{f}$-reducing polynomial, so

$$\bar{f} = (1\ 0\ 1\ 1\ 0\ 0\ 1\ 1,\ 1\ 0\ 0\ 0\ 1\ 1\ 1)\ (1\ 0\ 1\ 1\ 0\ 0\ 1\ 1,\ 1\ 0\ 0\ 0\ 1\ 1)$$

must be a nontrivial factorization:

```
1 0 1 1 0 0 1 1                1 0 1 1 0 0 1 1
1 0 0 0 1 1 1                  1 0 0 0 1 1
---------------                ---------------
    1 1 1 1 0 1                    1 1 1 1 1 1
    1 0 0 0 1 1 1                  1 0 0 0 1 1
    -------------                  -----------
      1 1 1 1 0 1                    1 1 1 0 0
      1 1 1 1 0 1                    1 0 0 0 1 1
                                     -----------
                                       1 1 0 1 1
                                         1 1 1
                                       ---------
                                           1 1 1
                                           1 1 1
                                           -----
```

Hence $\bar{f} = (1\ 1\ 1\ 1\ 0\ 1)\ (1\ 1\ 1)$. Of course 1 1 1 is irreducible, and it remains to investigate 1 1 1 1 0 1. The matrix of even powers modulo 1 1 1 1 0 1 is obtained by reducing the corresponding matrix for $\bar{f}$ by reducing mod 1 1 1 1 0 1:

$$\begin{aligned} x^0 &= 0\ 0\ 0\ 0\ 1 \\ x^2 &= 0\ 0\ 1\ 0\ 0 \\ x^4 &= 1\ 0\ 0\ 0\ 0 \\ x^6 &= 0\ 0\ 1\ 1\ 1 \\ x^8 &= 1\ 1\ 1\ 0\ 0 \end{aligned}$$

$$\begin{array}{ll} x & = 0\ 0\ 0\ 1\ 0 \\ x^2 & = 0\ 0\ 1\ 0\ 0 \\ x^4 & = 1\ 0\ 0\ 0\ 0 \\ x^8 & = 1\ 1\ 1\ 0\ 0 \\ x^{16} & = 0\ 1\ 0\ 1\ 1 \\ \hline T_1(x) & = 0\ 0\ 0\ 0\ 1 \\ \multicolumn{2}{c}{x^{25} = x,\ N = 5} \end{array} \qquad \begin{array}{ll} x^3 & = 0\ 1\ 0\ 0\ 0 \\ x^6 & = 0\ 0\ 1\ 1\ 1 \\ x^{12} & = 1\ 0\ 1\ 0\ 1 \\ x^{24} & = 0\ 1\ 1\ 0\ 1 \\ x^{48} & = 1\ 0\ 1\ 1\ 0 \\ \hline T_3(x) & = 0\ 0\ 0\ 0\ 1 \end{array}$$

Hence 1 1 1 1 0 1 is irreducible and so $\bar{f}(x) = (1\ 1\ 1\ 1\ 0\ 1)\ (1\ 1\ 1)$ is a product of irreducibles. (Actually in this case we could deduce that 1 1 1 1 0 1 was irreducible from $N = 10$ for $\bar{f}$, since any factorization of 1 1 1 1 0 1 would have led to a different N.) Next we check to see whether or not (f, f') is divisible by either of the two factors already found. $(f, f') = (1\ 1\ 0\ 0\ 0\ 1)^2$, so we need only check for divisibility by 1 1 1, and it is easily found that $1\ 1\ 0\ 0\ 0\ 1 = (1\ 1\ 1)\ (1\ 0\ 1\ 1)$. Hence

$$f(x) = (x^5 + x^4 + x^3 + x^2 + 1)(x^3 + x + 1)^2(x^2 + x + 1)^3$$

is the complete factorization.

2. Consider the factorization of the polynomials $x^e - 1$ over $GF(p)$, p a prime. There is no loss in assuming that $(e, p) = 1$, since if $e = e_1 p^t$, then $x^e - 1 = (x^{e_1} - 1)^{p^t}$. In this special case, the computation of the R_i is very simple (see proof of Lemma 1); one need only compute the orbits of the residues mod e under the cyclic permutation group generated by $i \to ip \pmod{e}$, and these orbits contain the exponents which occur in the various R_i. For example with $p = 3$, $e = 20$ the orbits are

$$(0),\ (1, 3, 9, 7)\ (2, 6, 18, 14)\ (4, 12, 16, 8)\ (5, 15)\ (10)\ (11, 13, 19, 17),$$

and so the corresponding R_i are $R_1(x) = x + x^3 + x^7 + x^9$, $R_2(x) = x^2 + x^6 + x^{14}$

$+ x^{18}$; $R_3(x) = x^4 + x^8 + x^{12} + x^{16}$, etc. The algorithm of this paper, using the R_i's, was programmed on an SDS-930 computer, and produced the table appearing in the microfiche section of this issue.

Notes on the Table in the Microfiche Section: For a given e only the irreducible factors of $x^e - 1$ which are not factors of $x^{e'} - 1$ for $e' < e$ are given, so what we have really is a table of the factorization of the *cyclotomic* polynomials $\Phi_e(x)$ of order e, $\deg \Phi_e(x) = \phi(e)$. The complete factorization is obtained from the formula $x^e - 1 = \prod_{d|e} \Phi_d(x)$. As is well known, the irreducible factors of $\Phi_e(x)$ are all of the same degree $= \operatorname{ord}_e(p)$, and in fact the shape of the complete factorization may be seen from the orbits used to calculate the R_i. In the example given above, the orbit structure shows that $x^{20} - 1$ is a product of four irreducibles of degree 4, one of degree 2 and two of degree one. The orbits (1, 3, 9, 7) and (11, 13, 19, 17) exhaust the residues prime to 20, so that $\Phi_{20}(x)$ is a product of two irreducibles of degree 4.

If a polynomial $f(x) = a_0 + a_1x + \cdots + a_mx^m$ divides $\Phi_e(x)$, then so does its reciprocal polynomial $\tilde{f}(x) = a_m + a_{m-1}x + \cdots + a_0x^m$, and only one member of a reciprocal pair is listed. For those e which divide an integer of the form $p^t + 1$, each irreducible divisor of $\Phi_e(x)$ is self-reciprocal; this is indicated by a "P" (since the polynomials are then *palindromes*) after the entry e. When e is either an odd prime r (or twice an odd prime) and $\Phi_e(x) = x^{r-1} + x^{r-2} + \cdots + x + 1$ (or $x^{r-1} - x^{r-2} + \cdots - x + 1$) is irreducible, the entry "I" is given. Also, for some values of $e = fg$ the irreducible divisors of $\Phi_e(x)$ may be obtained from those of period f by replacing x by x^g. This is indicated by the entry $(f \cdot g)$.

Finally, for $p = 2$ and 3 the entries are coded. Binary polynomials are given the customary octal representation; e.g., 7053 represents $x^{11} + x^{10} + x^9 + x^5 + x^3 + x + 1$. Ternary polynomials are coded in the base 9; e.g., 378 represents $x^5 + 2x^3 + x^2 + 2x + 2$. Polynomials for $p = 5$ and $p = 7$ are not coded; i.e., the coefficients are read directly from the table entries.

Information Processing
Jet Propulsion Laboratory
Pasadena, California 91103

1. R. W. MARSH, *Table of Irreducible Polynomials over GF(2) through Degree* 19, NSA, U.S. Department of Commerce, Office of Tech. Service, Washington, D.C., 1951.
2. E. R. BERLEKAMP, "Factoring polynomials over finite fields," *Bell System Tech. J.*, v. 46, 1967, pp. 1853–1859. MR **36** #2314.
3. S. LANG, *Algebra*, Addison-Wesley, Reading, Mass., 1965. MR **33** #5416.

Table of Polynomials of Period e over GF(p)

p=2:

e	factors
3	I
5	I
7	13
9	(3·3)
11	I
13	I
15	31
17P	471,727
19	I
21	165
23	5343
25	(5.5)
27	(3.9)
29	I
31	75,73,45
33P	3043,2251
35	16475
37	I
39	17075
41P	5747175,6647133
43P	64213,47771,52225
45	(15.3)
47	43073357
49	(7.7)
51	637,661
53	I
55	7164555
57P	1735357,1341035
59	I
61	I
63	147,141,155
65P	15353,13535,12345,10761
67	I
69	34603145
71	503700420663
73	1401,1641,1511,1145
75	(15.5)
77	16471647235
79	11435717264067
81	(3.27)
83	I
85	771,613,735,675
87	3706175715
89	6061,7773,7571,7311
91	14015,15713,11721
93	3205,3247,2065
95	1435137342601

e	factors
97P	10265044102212641, 17441554343330237
99	(33.3)
101	I
103	13070247640757l413
105	15611,13321
107	I
109P	1633437743547 1253417703525 1311255325115
111	1474435670631
113P	3367163573 2330160331 2427043505 2064774541
115	762131040775605
117	17741,17367,15035
119	162732025,112530321
121	(11.11)
123	7373121,5746331
125	(5.25)
127	375,361,301,367,313,325 345,271,221
129P	77277,62723,71747,41241, 51745,42721
131	I
133	1734415,1532007,1334325
135	(15.9)
137P	56473116332226634467135 67357330373267606675673
139	I
141	32022315576054461
143	145236760547324505061
145P	3572445367,2634370715 2045776441,2153567261
147	(21.7)
149	I
151	142327,166761,154253, 117431,115455
153	(51.3)
155	6234255,6441547,4454725
157P	352125723713652127 200233271635331001 235566252525156671
159	303667410520590411
161	150536353761,132352461225
163	I

e	factors
165	6223427,6130725
167	5122622544667121565742432523
169	(13.13)
171P	1635347,1505213,1341035 1315315,1167671,1331155 1055321
173	I
175	(35..5)
177P	31156240456440516623 23563311065422331671
179	I
181	I
183	174717374702233410115
185P	14770311141763 17615577733077 1544627646233 1170515312171
187	36000132706473 36347534660115
189	(63.3)
191	4021026115635307552216- 1226634177
193P	10206534661057031141721- 0663528041, 1740302577277055533217- . 65772414037
195	17657,16701,15347,12601
197	I
199	132370427053005723136255- 5070462553
201P	17700735637357473560177 13366124124762502506755
203	1647235164723516472351647235
205P	7632637,7037607,6727273, 5442115,4562351,5327265, 5047105,4057501
207	(69.3)
209P	1521141602464351134262407031053, 1152241145135375375351231024531
211	I
213	357117402363040717553625
215	3657555473,3351404305, 2742762331
217	163431,162405,151265,112305, 137325,107501
219	1600401,1512641,1654501, 1052465
221	171544505,142774525, 152003001,11176011
223	3705317547055,3552504574013, 2637116550561
225	(15.15)
227	I
229P	34604254444677544446504147 24455336006237114017326445 27527663640516240571575275
231	15051344155,11274767701
233	6241072161,6626630775, 6704436621,5766241661
235	6244662420377503553701674734421
237	152377515452522451517276321
239	422123214143045700106420- 0331223063324217
241P	141377503,143610743,161676707, 150153013,163276547,130753615, 132777655,114135031,103377541, 123252545
243	(3'81)
245	(35·7)
247	1440476534657,1617202471651, 1233142314101
249P	3607140011264370552200063417, 2755361003707657437002172675

p=3

n	factors
2	I
4	(2 2)
5	I
7	I
8	15
10	I
11	378
13	45,38
14	I
16	(8.2)
17	I
19	I
20	137
22	387
23	322158
25	(5.5)
26	37,47
28P	1334,1667
29	I
31	I
32	(8.4)
34	I
35	1853511
37P	1226303821 1578282784
38	I
40	141,171
41P	11541,12351, 14214,15024
43	I
44	(22.2)
46	546331, 456332
47	431416612362
49	(7.7)
50	(10.5)
52	(26.2)
53	I
55	11870256487
56	1242,1608
58	I
59	46624482624874 2
61P	104431,116671,125551,155854, 158284,176377
62	I
64	(8.8)
65	1543667,1725141
67P	132866368804 141326380414 170066066017

n	factors
68	162802504
70	1126884
71	30012213868756 2888
73P	1105311,1140141,1500024, 1634337,1743447,1806627
74P	1223606521,1845252457
76P	1326443804,1623776507
77	1187352778301187
79	I
80	105,185,108,148
82P	17217,18027,15354,11871,12681
83	377073178088048512078
85	162674324,174108711
86	I
88	103275,106248
89	I
91	1131,1247,1374,1377,1517,1561
92	(46.2)
94	532526621361
95	10347050720154531 67
97P	103757783422452135778 4631 140423037628128076305 1314
98	(14.7)
100	(20.5)

p=5

n	factors
2	I
3	I
4	12
6	I
7	I
8	(4.2)
9	(3.3)
11	124114
12	124
13P	13031,12121,11411
14	I
16	(4.4)
17	I
18	(6.3)
19	103222424
21P	1431341,1022201
22	114431
23	I
24	112,123
26P	12021,13131,14441
27	(3.9)
28	1243124
29P	144224030422441 124044313440421
31	1014,1024,1114,1134,1214
32	(4.8)
33	11214134031
34	I
36	(12.3)
37	I
38	1033234341
39	10141,10221,11321
41P	1002033310201333O2001 111441240434042144111
42P	1022201,1023201,1134311
43	I
44	111212,121232
46	I
47	I
48	(24.2)
49	(7.7)

p=7

n	factors
2	I
3	13
4	(2.2)
5	I
6	12
8P	131,141
9	(3.3)
10	I
11	I
12	(6.2)
13	I
15	12412
16	116,136
17	I
18	(6.3)
19	1026,1336,1416
20	13441
22	I
23	I
24	114,152
25P	12421,14041,14341,15551,16561
26	I
27	(3.9)
29	11530016,12505616
30	13264
31	1366341204313626
32	(16.2)
33	12412412412
34	I
36	(6.6)
37	1003442256,1012226316
38	1021,1131,1341
39	1241241241241
40	11631,14661
41	I
43P	1022201,1046401,1135311,1416141, 1550551,1602061,1643461
44P	12526562521,15556265551
45	(15.3)
46	I
47	123454362520440342500016
48	113,123,125,145
50P	11521,12521,13031,13331,15451

ON LEHMER"S METHOD

FOR FINDING THE ZEROS OF A POLYNOMIAL

PL/I Program

by

G. W. STEWART III

```
LEHMER: PRØCEDURE(AA,Z,CØND,NN);

        /* LEHMER FINDS THE ZERØS ØF THE PØLYNØMIAL ØF DEGREE NN
           WHØSE CØEFFICIENTS ARE CØNTAINED IN THE ARRAY AA  .
           BY A MØDIFICATIØN ØF LEHMER'S METHØD.  THE APPRØXIMATE
           ZERØS ARE RETURNED IN THE ARRAY Z.  WITH EACH ZERØ THE
           PRØCEDURE RETURNS A CØNDITIØN NUMBER IN THE ARRAY
           CØND.  FØR SIMPLE ZERØS THE PRØDUCT OF THIS NUMBER AND
           THE RELATIVE PRECISIØN ØF THE ARITHMETIC MAY GIVE
           AN INDICATIØN ØF THE ABSØLUTE ACCURACY ØF THE
           APPRØXIMATE ZERØ.

        DECLARE ((AA,Z)(*),(A,B,C)(0:NN),(S,DELTAS,SK) STATIC)
                CØMPLEX(16),(R,RP,ØLDR) STATIC REAL(16),CØND(*)
                (CØNS INIT(1.625),
                 CØNR INIT(0.875),
                 BIGØMEGA INIT(1.E75),
                 UNIT(8) CØMPLEX(16) INIT
                 (+1.0000 + 0.0000I,
                  +0.7071 - 0.7071I,
                  +0.7071 + 0.7071I,
                  +0.0000 - 1.0000I,
                  -0.0000 + 1.0000I,
                  -0.7071 - 0.7071I,
                  -0.7071 + 0.7071I,
                  -1.0000 - 0.0000I )) STATIC,
                CØHN ENTRY RETURNS(BIT(1)),
                FUNDER ENTRY(,,,,FIXED BINARY);

 SETUP: /* INITIALIZE THE PRØGRAM TØ IGNØRE UNDERFLØWS AND SCALE
           THE CØEFFICIENTS SØ THAT THE PØLYNØMIAL IS MØNIC.
           *
        ØN UNDERFLØW;
        DØ I=0 TØ NN; A(I)=AA(I)/AA(NN); END;
        N = NN;
        ØLDR = 0;

 START: /* DETERMINE AN INITIAL ANNULUS ABØUT THE ØRIGIN.  IF NØ
           PREVIØUS ZERØ HAS BEEN FØUND CALCULATE THE STARTING
           RADIUS.  ØTHERWISE USE THE ØUTER RADIUS OF THE ØLD
           ANNULUS.
           *
        S = 0;
```