POLYNOMIAL DIVISIBILITY IN FINITE FIELDS, AND RECURRING SEQUENCES

Odoardo Brugia and Piero Filipponi

Fondazione Ugo Bordoni, Via B. Castiglione 59, I-00142 Rome, Italy

(*Submitted May 1994*)

1. INTRODUCTION AND PRELIMINARIES

The theory of polynomials the coefficients of which belong to finite fields (e.g., see [4]) is a valid mathematical tool to face various problems arising in telecommunication engineering. For example, it plays a crucial role in the design of scramblers and descramblers, multilevel co-decoders, linear shift-registers, etc., and in the analysis of their performances (e.g., see [1], [5]). It is sometimes necessary to fix our attention on special classes of these polynomials, such as *irreducible* and *primitive* polynomials [4], [5]. For example, for the sequence generated by a linear feedback shift register to be of maximal length, the characteristic polynomial of the register must be primitive [1], [2].

To seek irreducible polynomials or to factor reducible ones, it is useful to have at disposal criteria for the divisibility over the finite field GF(q) (q a prime or a power of a prime) of a polynomial $f(x)$ by a polynomial $g(x)$ of degree less than that of $f(x)$. Some criteria for the divisibility over GF(2) are well known. As a minor instance, we have that: (i) if the coefficient of the zero-degree term of $f(x)$ vanishes, then this polynomial is divisible by its term of lower degree; (ii) if the number of the nonzero coefficients is even, then $f(x)$ is divisible by $x+1$.

Following the notation of Lidl [4], let $f(x)\in \mathrm{GF}(q)[x]$ and $g(x)\in \mathrm{GF}(q)[x]$ be two polynomials of arbitrary degree n and m ($m<n$), respectively,

$$f(x)=\sum_{k=0}^{n}a_kx^k,\ a_k\in \mathrm{GF}(q),\ a_n\not\equiv 0 \pmod q, \tag{1.1}$$

$$g(x)=x^m-\sum_{k=0}^{m-1}b_kx^k,\ m<n,\ b_k\ \mathrm{GF}(q). \tag{1.2}$$

The polynomial $f(x)$ is divisible in GF(q) by $g(x)$ if the remainder of $f(x):g(x)$ is congruent to zero modulo q. In Section 2, criteria for this divisibility are established which involve the use of certain m^{th}-order recurring sequences. The ubiquitous Fibonacci numbers make their appearance in the case $m=q=2$. In Section 3, three special cases are analyzed, the last of which turns out to be a useful tool for ascertaining the irreducibility or the primitivity of certain classes of polynomials.

Throughout this paper, all relations and algebraic manipulations are meant to be performed modulo q. This fact will be indicated explicitly only in the final results.

2. THE MAIN RESULT

The (provisional) remainder $f_i(x)$ obtained at the i^{th} step ($0\le i\le n-m+1$) of the long division $f(x):g(x)$ has the form

$$f_i(x) = \sum_{j=0}^{n-i} r_j^{(i)} x^{n-i-j}, \; r_j^{(i)} \in \mathrm{GF}(q). \tag{2.1}$$

Obviously, the *actual* remainder of this division is $f_{n-m+1}(x)$. Moreover, we assume that $f_0(x) = f(x)$, which implies

$$r_j^{(0)} = a_{n-j} \quad (j = 0, 1, \ldots, n). \tag{2.2}$$

Since the term of $(n-i-m)^{\text{th}}$-degree of the quotient is given by $r_0^{(i)} x^{n-i-m}$, using the long division algorithm gives the $(i+1)^{\text{th}}$ provisional remainder

$$f_{i+1}(x) = f_i(x) - r_0^{(i)} x^{n-i-m} g(x) = \sum_{j=0}^{n-i-1} \left(r_{j+1}^{(i)} + b_{m-j-1} r_0^{(i)} \right) x^{n-i-j-1}, \tag{2.3}$$

whereas, by definition (2.1), we can write

$$f_{i+1}(x) = \sum_{j=0}^{n-i-1} r_j^{(i+1)} x^{n-i-j-1}. \tag{2.4}$$

By identifying the terms of the same degree in (2.3) and (2.4), the following system of $n-i$ difference equations can be written

$$r_j^{(i+1)} = \begin{cases} r_{j+1}^{(i)} + b_{m-j-1} r_0^{(i)} & (0 \le j \le m-1), \\ r_{j+1}^{(i)} & (m \le j \le n-i-1), \end{cases} \tag{2.5}$$

the initial conditions of which are given by (2.2).

By (2.2), the second equation of (2.5) produces

$$\begin{aligned} & r_j^{(1)} = r_{j+1}^{(0)} = a_{n-j-1}, \\ & r_j^{(2)} = r_{j+1}^{(1)} = r_{j+2}^{(0)} = a_{n-j-2}, \\ & r_j^{(3)} = r_{j+1}^{(2)} = r_{j+2}^{(1)} = r_{j+3}^{(0)} = a_{n-j-3}, \\ & \ldots \\ & r_j^{(i)} = r_{j+1}^{(i-1)} = \cdots = a_{n-j-i} \quad (m \le j \le n-i-1), \end{aligned} \tag{2.6}$$

whence, as a special case,

$$r_m^{(i)} = a_{n-m-i}. \tag{2.6'}$$

The first equation of (2.5) produces the equations

$$\begin{aligned} & r_j^{(i)} = r_{j+1}^{(i-1)} + b_{m-j-1} r_0^{(i-1)}, \\ & r_{j+1}^{(i-1)} = r_{j+2}^{(i-2)} + b_{m-j-2} r_0^{(i-2)} \\ & \ldots \\ & r_{m-1}^{(i-m+j+1)} = r_m^{(i-m+j)} + b_0 r_0^{(i-m+j)}. \end{aligned}$$

Summing both sides of these equations and using (2.6′) yields

$$r_j^{(i)} = r_m^{(i-m+j)} + \sum_{\ell=1}^{m-j} b_{m-j-\ell} r_0^{(i-\ell)} = a_{n-i-j} + \sum_{\ell=1}^{m-j} b_{m-j-\ell} r_0^{(i-\ell)} \quad (0 \le j \le m-1). \tag{2.7}$$

For $j=0$; (2.7) reduces to

$$r_0^{(i)} = a_{n-i} + \sum_{\ell=1}^{m} b_{m-\ell} r_0^{(i-\ell)}, \tag{2.8}$$

where $r_0^{(i-\ell)} = 0$ if $i < \ell$, and (2.2) applies.

Proposition 1:

$$r_0^{(i)} = \sum_{h=0}^{i} a_{n-h} Z_{i-h+1}, \tag{2.9}$$

where the integers Z_h obey the recurrence

$$Z_h = b_{m-1}Z_{h-1} + b_{m-2}Z_{h-2} + \cdots + b_0 Z_{h-m} \tag{2.10}$$

which is of m^{th}-order if $b_0 \not\equiv 0 \pmod{q}$, and has initial conditions

$$Z_h = 0 \text{ (for } -m+2 \le h \le 0) \text{ and } Z_1 = 1 \tag{2.11}$$

or, equivalently,

$$\begin{cases} Z_1 = 1, \\ Z_2 = b_{m-1}Z_1, \\ Z_3 = b_{m-1}Z_2 + b_{m-2}Z_1, \\ \cdots \\ Z_m = b_{m-1}Z_{m-1} + b_{m-2}Z_{m-2} + \cdots + b_1 Z_1. \end{cases} \tag{2.11$'$}$$

Proof: We shall prove that replacing the right-hand side of (2.9) in (2.8) yields an identity. In fact, this replacement gives the equation

$$\begin{aligned} \sum_{h=0}^{i} a_{n-h} Z_{i-h+1} = a_{n-i} + b_{m-1} \sum_{h=0}^{i-1} a_{n-h} Z_{i-h} \\ + b_{m-2} \sum_{h=0}^{i-2} a_{n-h} Z_{i-h-1} + \cdots + b_0 \sum_{h=0}^{i-m} a_{n-h} Z_{i-h-m+1}. \end{aligned} \tag{2.12}$$

By reducing all summations in (2.12) to the same upper range indicator (namely, $i-m$), we can write

$$\begin{aligned} & a_{n-i}Z_1 + a_{n-i+1}Z_2 + \cdots + a_{n-i+m-1}Z_m + \sum_{h=0}^{i-m} a_{n-h}Z_{i-h+1} \\ &= a_{n-i} + b_{m-1}(a_{n-i+1}Z_1 + a_{n-i+2}Z_2 + \cdots + a_{n-i+m-1}Z_{m-1}) + b_{m-1}\sum_{h=0}^{i-m} a_{n-h}Z_{i-h} \\ &+ b_{m-2}(a_{n-i+2}Z_1 + \cdots + a_{n-i+m-1}Z_{m-2}) + b_{m-2}\sum_{h=0}^{i-m} a_{n-h}Z_{i-h-1} + \cdots \\ &+ b_1(a_{n-i+m-1}Z_1) + b_1 \sum_{h=0}^{i-m} a_{n-h}Z_{i-h-m+2} + b_0 \sum_{h=0}^{i-m} a_{n-h}Z_{i-h-m+1}. \end{aligned}$$

The above equation can be rewritten as

$$a_{n-i}(Z_1-1)+a_{n-i+1}(Z_2-b_{m-1}Z_1)+\cdots+a_{n-i+m-1}(Z_m-b_{m-1}Z_{m-1}-\cdots-b_1Z_1)$$
$$+\sum_{h=0}^{i-m}a_{n-h}(Z_{i-h+1}-b_{m-1}Z_{i-h}-b_{m-2}Z_{i-h-1}-\cdots-b_0Z_{i-m-h+1})=0,$$

which, by (2.10) and (2.11′) is identically satisfied. Q.E.D.

Recalling that the quantities $r_j^{(n-m+1)}$ ($j=0,1,\ldots,m-1$) are the coefficients of the remainder of $f(x):g(x)$, it becomes patent that $f(x)$ is divisible by $g(x)$ iff $r_j^{(n-m+1)}\equiv 0\ (\mathrm{mod}\ q)$ for *all* admissible values of j. By (2.9), after some simple manipulations, one can see that the condition $r_0^{(n-m+1)}\equiv 0\ (\mathrm{mod}\ q)$ is satisfied if

$$\sum_{h=m-1}^{n}a_hZ_{h-m+2}\equiv 0\ (\mathrm{mod}\ q). \tag{2.13}$$

By using the first equation of (2.5), we can get analogous conditions pertaining to $r_j^{(n-m+1)}$ for $1\le j\le m-1$. For example, letting $j=0$ in (2.5) yields

$$r_1^{(n-m+1)}=r_0^{(n-m+2)}-b_{m-1}r_0^{(n-m+1)}\equiv r_0^{(n-m+2)}\ (\mathrm{mod}\ q)\quad [\text{by } (2.13)],$$

whence, by (2.9), the condition $r_1^{(n-m+1)}\equiv r_0^{(n-m+2)}\equiv 0\ (\mathrm{mod}\ q)$ is satisfied if

$$\sum_{h=m-2}^{n}a_hZ_{h-m+3}\equiv 0\ (\mathrm{mod}\ q). \tag{2.14}$$

Iterating this procedure for all values of j allows us to state our main result.

Proposition 2 (main result): The polynomial $f(x)$ is divisible by the polynomial $g(x)$ iff

$$\sum_{h=m-j-1}^{n}a_hZ_{h-m+j+2}\equiv 0\ (\mathrm{mod}\ q)\ \text{for } j=0,1,\ldots,m-1. \tag{2.15}$$

3. SPECIAL CASES

For small values of m, or for special polynomials $f(x)$, the divisibility conditions (2.15) simplify remarkably. In this section, three special cases are discussed in detail.

Case 1: $m = 1$

If $m=1$, Proposition 2 tells us that $f(x)$ is divisible by $x-b_0$ [$b_0\not\equiv 0\ (\mathrm{mod}\ q)$] iff

$$\sum_{h=0}^{n}a_hZ_{h+1}\equiv\sum_{h=0}^{n}a_hb_0^h\equiv 0\ (\mathrm{mod}\ q), \tag{3.1}$$

since $Z_h=b_0Z_{h-1}$ with $Z_1=1$ [see (2.10)-(2.11)] implies $Z_h=b_0^{h-1}$. The condition (3.1) agrees with the well-known fact (e.g., see [4], Theorem 1.64) that, if $f(b_0)\equiv 0\ (\mathrm{mod}\ q)$, then $f(x)$ is divisible by $x-b_0$ [cf. point (ii) in Section 1].

Case 2: $m = 2$

If $m=2$, Proposition 2 tells us that $f(x)$ is divisible by $x^2-b_1x-b_0$ [$b_0\not\equiv 0\ (\mathrm{mod}\ q)$] iff

$$\sum_{h=1-j}^{n} a_h Z_{h+j} \equiv 0 \pmod{q} \quad (j=0,1), \tag{3.2}$$

where the numbers Z_h are the *generalized Fibonacci numbers* W_h [more precisely, the numbers $W_h(b_1, -b_0;\, 0, 1)$] which have been studied extensively over the past years (e.g., see [3] for background material). In particular, if $q = 2$, $f(x)$ is divisible by $x^2 - x - 1$ iff

$$\sum_{h=1-j}^{n} a_h F_{h+j} \equiv 0 \pmod{2} \quad (j=0,1), \tag{3.3}$$

where F_h denotes the h^{th} Fibonacci number. Taking into account that F_h is even iff $h \equiv 0 \pmod{3}$, conditions (3.2) can be rewritten as

$$\sum_{\substack{h=1 \\ h\not\equiv 0 \,(\mathrm{mod}\, 3)}}^{n} a_h \equiv \sum_{\substack{h=1 \\ h\not\equiv 2 \,(\mathrm{mod}\, 3)}}^{n} a_h \equiv 0 \pmod{2}. \tag{3.4}$$

Case 3: $f(x) = x^n - 1$

If $f(x) = x^n - 1$, then Proposition 2 tells us that $f(x)$ is divisible by $g(x)$ iff

$$\begin{cases} Z_{n-m+j+2} \equiv 0 \pmod{q} \quad (j = 0, 1, \ldots, m-2), \\ Z_{n+1} \equiv Z_1 \equiv 1 \pmod{q}. \end{cases} \tag{3.5}$$

When $n = q^m - 1$ and m is a prime not less than q, the fulfillment of (3.5) implies that $g(x)$ [$b_0 \not\equiv 0 \pmod{q}$] is *irreducible* (see [4], Theorem 3.20). Moreover, if $q = 2$ and n is a Mersenne prime, then $g(x)$, beyond being irreducible, is *primitive* (see [4], Corollary 3.4).

The fulfillment of (3.5) can be checked out rapidly by means of the software implementation of an m-cell linear feedback shift register [2] having $g(x)$ as its characteristic polynomial, and initial state [1, 0, 0, ..., 0]. Once this is made, one simply has to ascertain that the m terms $Z_{n-m+2}, Z_{n-m+3}, \ldots, Z_{n+1}$ of the sequence $\{Z_h\}$ generated by this device satisfy (3.5).

ACKNOWLEDGMENT

This work has been carried out in the framework of an agreement between the Italian PT Administration (Istituto Superiore PT) and the Fondazione Ugo Bordoni.

REFERENCES

1. H. Beker & F. Piper. *Cipher Systems*. New York: Wiley, 1982.
2. S. W. Golomb. *Shift Register Sequences*. Laguna Hills, Calif.: Aegean Park Press, 1982.
3. A. F. Horadam. "Generalization of a Result of Morgado." *Portugaliae Mathematica* **44.2** (1987):131-36.
4. R. Lidl & H. Niederreiter. "Finite Fields." In *Encyclopedia of Mathematics and Its Applications*. Vol. 20. Ed. Gian-Carlo Rota. Reading, Mass.: Addison Wesley, 1983.
5. W. W. Peterson. *Error-Correcting Codes*. New York: Wiley, 1961.

AMS Classification Numbers: 12E05, 11B83, 11B39