# POLYNOMIAL FACTORIZATION IN GF ($2^m$).

**Y.Z. Boutros, G.P. Fiani, E.S. Looka**
Alexandria University, Alexandria, Egypt.

ABSTRACT

**Polynomial factorization in the finite Galois field GF ($2^m$) is the basis of the design of good error correcting codes. In this paper, a simple algorithm for polynomial factorization in GF($2^m$) is proposed. Interesting properties of prime polynomial factors are deduced.**

*Keywords*

Polynomial factorization, Error correcting codes.

## 1.INTRODUCTION

In recent years, Galois fields (GF) have received attention in the area of communications, with applications in error correcting codes [1-3] and cryptography [4]. The finite field GF ($2^m$) contains $2^m$ elements which can be represented in several forms. Although all calculations are carried mod 2, and no carries are involved, GF ($2^m$) arithmetic is a complex and difficult task. Recently, Yeh, Reed, and Truong [5] have developed systolic architectures for performing the operation ABC in GF($2^m$) that are suitable for use in VLSI systems.

Polynomial factorization in GF($2^m$) is used in the design of good error correcting codes. The common approach is to compute the GCD of several polynomials over a finite field using direct commands in MACSYMA or in MAPLE software mathematical packages.

In the present paper we introduce a new simple and easy to implement recursive algorithm for polynomial factorization in GF($2^m$). Computer results are in agreement with previous published results [6,7]. Some interesting properties of prime polynomials are deduced.

## 2. POLYNOMIAL FACTORIZATION IN GF($2^m$)

Given the polynomial f(x) of order n,

$$f(x) = \sum_{i=0}^{m} a_i x^i ; a_i \in GF(2),$$

it is required to determine the prime factor polynomials of f(x) in GF($2^m$); all operations are carried mod 2.

We define the decimal equivalent of f(x) as a decimal value F obtained by substituting for x the value 2 so that

$$F = \sum_{i=0}^{m} a_i 2^i$$

A prime factor polynomial p (x) in GF($2^m$) is defined as a polynomial that is irreducible in GF($2^m$). A list of all prime polynomials of orders up to 8 is given in Table I. The polynomials are written in their decimal equivalent.

The steps of the proposed factorization algorithm are as follows:

1. INITIALIZATION.

A list of all prime polynomials of order up to n-1 should be available. If not, the algorithm is capable of generating such a list iteratively as explained in 7.

2. *CASE I. Direct Polynomial Factorization.*

We calculate F, the decimal equivalent of f(x).
For any prime polynomial p(x) of degree less than n, with decimal equivalent P, if F is divisible by P, then p(x) is a factor of f(x) and F can be put in the form

$$F = H\,P, \qquad H > 1$$

where H is the quotient of F/P. Proceed to step 6.

3. CASE II. Augmented Polynomial Factorization.

If no prime polynomial satisfies the condition in step 2, we check all possible missing terms in f(x) due to multiplication in GF(2). A typical missing term is 2X in which the coefficient 2 is equivalent to 0 in GF(2). We construct an augmented form of f(x), denoted by g(x), by adding to f(x) all different combinations of all middle terms multiplied by 2 as follows:

$$g(x) = f(x) + \sum_{i=1}^{m-1} 2\, b_i\, x^i \; ; b_i \in GF(2)$$

$$= \sum_{i=0}^{m} a_i x^i + \sum_{i=1}^{m-1} 2 b_i x^i \; ; a_i, b_i \in GF(2)\,..$$

We then calculate the decimal equivalent of g(x) denoted by G.

4. If G is divisible by P, the decimal equivalent of a prime polynomial p(x) of degree less than n, then we can write

$$G = H\,P, \qquad H > 1,$$

where H is the quotient of G/P. Proceed to step 6.

5. If both tests in steps 2 and 4 fail, i.e., neither F nor G are divisible by any of the prime polynomials of order less than n, then f(x) is a PRIME polynomial and the algorithm terminates prematurely. Otherwise, further factorization is required.
6. The prime polynomial p(x) corresponding to P is a prime factor of f(x). The resulting H has to be tested for further factorization using CASE I or CASE II. The algorithm stops if H=1, in which case, the polynomial f(x) has been completely factorized.
7. Note: This algorithm can be used to generate the list of all prime polynomials of order up to n-1 by trying to factorize all the $2^n$-1 polynomials in sequence, given that the first known prime polynomial is p(x)=x. The algorithm is repeated recursively for each polynomial and whenever a prime polynomial is obtained, it is added to the list.

**Table I.** A list of prime polynomial of orders up to 8.

Order : Prime polynomials
1 : 2,3
2 : 7
3 : 11,13
4 : 19,25,31
5 : 37,41,47,55,59,61
6 : 67,73,87,91,97,103,109,115,117
7 :131,137,143,145,157,167,171,185,191,
193,203,211,213,229
: 239,241,247,253 ,
8 : 261,283,285,299,301,313,319,333,341,351,
355,357,361,369,357,379,391,397,415,419,425,
433,445,451,463,471,477,487,499,501,505

To clarify the algorithm, we give in the following the partial results and final factorization of all the polynomials f(x) of order at most 3, (i.e. n=3)

| Order | f(x) | g(x) | decimal F | decimal G | factors | |
|---|---|---|---|---|---|---|
| 0 | 1 | | 1 | | PRIME | |
| 1 | X | | 2 | | PRIME | |
| 1 | 1+X | | 3 | | PRIME | |
| 2 | $X^2$ | | 4 | | 2, 2 | (X) (X) |
| 2 | 1 +$X^2$ | | 5 | | | |
| | | $1+2X+X^2$ | 9 | | 3, 3 | (1+X) (1+X) |
| 2 | $X+X^2$ | | 6 | | 2, 3 | (X) (1+X) |
| 2 | $1+X+X^2$ | | 7 | | PRIME | |
| 3 | $X^3$ | | 8 | | 2, 2, 2 | (X) (X) (X) |
| 3 | 1 +$X^3$ | | 9 | | | |
| | | 1+2X +$X^3$ | | 13 | | |
| | | 1 +$2X^2+X^3$ | | 17 | | |
| | | $1+2X+2X^2+X^3$ | | 21 | 3, 7 | $(1+X)(1+X+X^2)$ |
| 3 | X +$X^3$ | | 10 | | 2, 3, 3 | (X) (1+X) (1+X) |
| 3 | 1+X +$X^3$ | | 11 | | PRIME | |
| 3 | $X^2+X^3$ | | 12 | | 2, 2, 3 | (X) (X) (1+X) |
| 3 | 1 +$X^2+X^3$ | | 13 | | PRIME | |
| 3 | $X+X^2+X^3$ | | 14 | | 2, 7 | $(X)(1+X+X^2)$ |
| 3 | $1+X+X^2+X^3$ | | 15 | | 3, 3, 3 | (1+X) (1+X) (1+X |

Table II gives the factorization of all polynomials of ord up to 8 with coefficients in GF(2) obtained by the prese algorithm. The polynomials are written in their decim equivalent.

**Table II.** Polynomial factorization for orders up to 8.

| | | | |
|---|---|---|---|
| | 64:2,2,2,2,2,2 | 128:2,2,2,2,2,2,2 | 192:2,2,2,2,2,2,3 |
| | 65:3,3,7,7 | 129:11,3 13 | 193:<-----PRIME |
| 2:<-----PRIME | 66:2,3 31 | 130:2,3,3,7,7 | 194:2 97 |
| 3:<----- PRIME | 67:< ----PRIME | 131:<-----PRIME | 195:3,3,3,7,7 |
| 4:2,2 | 68:2,2,3,3,3,3 | 132:2,2,3 31 | 196:2,2,7 11 |
| 5:3,3 | 69:11 11 | 133:7 55 | 197:3 67 |
| 6:2,3 | 70:2,7 13 | 134:2 67 | 198:2,3,3 31 |
| 7:< --PRIME | 71:3 61 | 135:3 25,3,3 | 199:13 19 |
| 8:2,2,2 | 72:2,2,2,3,7 | 136:2,2,2,3,3,3,3 | 200:2,2,2 25 |
| 9:3,[illegible] | 73:<-----PRIME | 137:<-----PRIME | 201:3,3 6[illegible] |
| 10:2,3,3 | 74:2 37 | 138:2 11 11 | 202:2,3,7 13 |
| 11:< PRIME | 75:3 13,3,3 | 139:3,7 19 | 203:<-----PRIME |
| 12:2,2,[illegible] | 76:2,2 19 | 140:2,2,7 13 | 204:2,2,3,3,3,3,3 |
| 13:< -PRIME | 77:3 59 | 141:41,3,3 | 205:7 47 |
| 14:2,7 | 78:2 11,3,3 | 142:2,3 61 | 206:2 103 |
| 15:[illegible],3,3 | 79:7 25 | 143:<-----PRIME | 207:3 11 11 |
| 16:2,2,2,2 | 80:2,2,2,2,3,3 | 144:2,2,2,2,3,7 | 208:2,2,2,2 13 |
| 17:3,3,3,3 | 81:13 13 | 145:<-----PRIME | 209:3,7 25 |
| 18:2,3,7 | 82:2 41 | 146:2 73 | 210:2,3 11,3,3 |
| 19:<-----PRIME | 83:3,7 11 | 147:47,3,3 | 211:<-----PRIME |
| 20:2,2,3,3 | 84:2,2,7,7 | 148:2,2 37 | 212:2,2,3 19 |
| 21:7,7 | 85:3,3,3,3,3,3 | 149:3 115 | 213:<-----PRIME |
| 22:2 11 | 86:2,3 25 | 150:2,3 13,3,3 | 214:2,7,7,7 |
| 23:3 13 | 87:<-----PRIME | 151:7,7 11 | 215:3,3 59 |
| 24:2,2,2,3 | 88:2,2,2 11 | 152:2,2,2 19 | 216:2,2,2,3,3,7 |
| 25:<-----PRIME | 89:3 55 | 153:3,7,3,3,3,3 | 217:11 31 |
| 26:2 3 | 90:2,3,3,3,7 | 154:2,3 59 | 218:2 109 |
| 27:3,3,7 | 91:<-----PRIME | 155:13 31 | 219:3 73 |
| 28:2,2,7 | 92:2,2,3 13 | 156:2,2 11,3,3 | 220:2,2 55 |
| 29:3 11 | 93:7 31 | 157:<-----PRIME | 221:13,3,3,3,3 |
| 30:2,3,3,3 | 94:2 47 | 158:2,7 25 | 222:2,3 37 |

| | | | |
|---|---|---|---|
| 31:<-----PRIME | 95:19,3,3 | 159:3 117 | 223:7 41 |
| 32:2,2,2,2,2 | 96:2,2,2,2,2,3 | 160:2,2,2,2,2,3,3 | 224:2,2,2,2,2,7 |
| 33:3 31 | 97:<-----PRIME | 161:7 59 | 225:3 19,3,3 |
| 34:2,3,3,3,3 | 98:2,7 11 | 162:2 13 13 | 226:2,3 47 |
| 35:7 13 | 99:3,3 31 | 163:3 97 | 227:11 25 |
| 36:2,2,3,7 | 100:2,2 25 | 164:2,2 41 | 228:2,2 13,3,3 |
| 37:<-----PRIME | 101:3,7 13 | 165:3,3,3 31 | 229:<-----PRIME |
| 38:2 19 | 102:2,3,3,3,3,3 | 166:2,3,7 11 | 230:2 115 |
| 39:11,3,3 | 103:<-----PRIME | 167:<-----PRIME | 231:3,7 31 |
| 40:2,2,2,3,3 | 104:2,2,2 13 | 168:2,2,2,7,7 | 232:2,2,2,3 11 |
| 41:<-----PRIME | 105:3 11,3,3 | 169:3 103 | 233:7,7 13 |
| 42:2,7,7 | 106:2,3 19 | 170:2,3,3,3,3,3,3 | 234:2 117 |
| 43:3 25 | 107:7,7,7 | 171:<-----PRIME | 235:3,3 55 |
| 44:2,2 11 | 108:2,2,3,3,7 | 172:2,2,3 25 | 236:2,2 59 |
| 45:3,3,3,7 | 109:<-----PRIM3 | 173:11 19 | 237:3 91 |
| 46:2,3 13 | 110:2 55 | 174:2 87 | 238:2,7,3,3,3,3 |
| 47:<-----PRIME | 111:3 37 | 175:3,3,7 13 | 239:<-----PRIME |
| 48:2,2,2,2,3 | 112:2,2,2,2,7 | 176:2,2,2,2 11 | 240:2,2,2,2,3,3,3 |
| 49:7 11 | 113:3 47 | 177:37,3,3 | 241:<-----PRIME |
| 50:2 25 | 114:2 13,3,3 | 178:2,3 55 | 242:2,7 19 |
| 51:3,3,3,3,3 | 115:<-----PRIME | 179:7 61 | 243:3 13 13 |
| 52:2,2 13 | 116:2,2,3 11 | 180:2,2,3,3,3,7 | 244:2,2 61 |
| 53:3 19 | 117:<-----PRIME | 181:13 25 | 245:3,3,7 11 |
| 54:2,3,3,7 | 118:2 59 | 182:2 91 | 246:2,3 41 |
| 55:<-----PRIME | 119:7,3,3,3,3 | 183:3 109 | 247:<-----PRIME |
| 56:2,2,2,7 | 120:2,2,2,3,3,3 | 184:2,2,2,3 13 | 248:2,2,2 31 |
| 57:13,3,3 | 121:7 19 | 185:<-----PRIME | 249:3 87 |
| 58:2,3 11 | 122:2 61 | 186:2,7 31 | 250:2 25,3,3 |
| 59:<-----PRIME | 123:3 41 | 187:11,3,3,3,3 | 251:7 37 |
| 60:2,2,3,3,3 | 124:2,2 31 | 188:2,2 47 | 252:2,2,3,7,7 |
| 61:<-----PRIME | 125:25,3,3 | 189:3,7,7,7 | 253:<-----PRIME |
| 62:2 31 | 126:2,3,7,7 | 190:2 19,3,3 | 254:2 11 13 |
| 63:3,7,7 | 127:11 13 | 191:<-----PRIME | 255:3,3,3,3,3,3,3 |

## 3. OBSERVATIONS.

From Table II and extensive computer runs, the following interesting properties were deduced.

1. If f(x) is a prime polynomial, then the reciprocal polynomial of f(x), i.e., the one with reversed bit order, is also a prime polynomial. Examples of polynomials, in decimal, having this property are 131 and 193, 137 and 145, 143 and 241, etc.
2. Up to a given order n, there exist $2^{n+1}$ -1 polynomials, of which, exactly $2^{n+1-d}$ - 1 polynomials have a common factor of order (d). To clarify this property, consider all polynomials of order at most 4,i.e., with $x^4$ being the highest order of x (31 polynomials). Consider also the prime factors (x), (1+x), $(1+x+x^2)$, $(1+x+x^3)$ and $(1+x^2+x^3)$, which correspond to the decimal values 2,3,7,11 and 13 and which are of order (d) 1,1,2,3 and 3 respectively. There exist out of the 31 polynomials exactly 15,15,7,3,1 and 1 having (x), (1+x), $(1+x+x^2)$, $(1+x+x^3)$ and $(1+x^2+x^3)$ respectively as common factors. Table IIIa illustrates this property.
3. The number of polynomials divisible by the product of two or more prime factor polynomials of overall order (d) follows the same rule mentioned in 2. Table IIIb shows the number of polynomials divisible by prime polynomial combinations.
4. Up to a given order n, there exist exactly (n/d) polynomials having one repeated factor of order (d), and no other factor. To clarify this property, consider all polynomials of order at most 4. There are exactly four polynomials that are factorized by (x) only, four by (1+x) only, two by $(1+x+x^2)$ only, one by $(1+x+x^3)$ and one by $(1+x^2+x^3)$. Table IIIc lists the number of polynomials having this property.

**Table III.** Properties of polynomial factorization.

(a) Number of polynomials divisible by a prime polynomial

| Polynomial Order | Total No. of Polyn. | Prime polynomials and their order 2:1 | 3:1 | 7:2 | 11:3 | 13:3 | 19:4 | 25:4 | 31:4 |
|---|---|---|---|---|---|---|---|---|---|
| 2 | 7 | 3 | 3 | 1 | - | | | | - |
| 3 | 15 | 7 | 7 | 3 | 1 | 1 | - | - | |
| 4 | 31 | 15 | 15 | 7 | 3 | 3 | 1 | 1 | 1 |
| 5 | 63 | 31 | 31 | 15 | 7 | 7 | 3 | 3 | 3 |
| 6 | 127 | 63 | 63 | 31 | 15 | 15 | 17 | 7 | 7 |
| 7 | 255 | 127 | 127 | 63 | 31 | 31 | 15 | 15 | 15 |
| 8 | 511 | 225 | 225 | 127 | 63 | 63 | 31 | 31 | 31 |

(b) Number of polunomials divisible by the prime polynomial combinations and the order of the product prime polynomials.

| Prime factor polyn. comb. | order | polynomials order (n) 2 | 3 | 4 | 5 | 6 | 7 | 8 |
|---|---|---|---|---|---|---|---|---|
| 2,3 | 2 | 1 | 3 | 7 | 15 | 31 | 63 | 127 |
| 2,7 | 3 | - | 1 | 3 | 7 | 15 | 31 | 63 |
| 3,7 | 3 | - | 1 | 3 | 7 | 15 | 31 | 63 |
| 2,3,7 | 4 | - | - | 1 | 3 | 7 | 15 | 31 |
| 2,11 | 4 | - | - | 1 | 3 | 7 | 15 | 31 |
| 3,11 | 4 | - | - | 1 | 3 | 7 | 15 | 31 |
| 2,13 | 4 | - | - | 1 | 3 | 7 | 15 | 31 |
| 3,13 | 4 | - | - | 1 | 3 | 7 | 15 | 31 |
| 2,3,11 | 5 | - | - | - | 1 | 3 | 7 | 15 |
| 7,11 | 5 | - | - | - | 1 | 3 | 7 | 15 |
| 2,3,13 | 5 | - | - | - | 1 | 3 | 7 | 15 |
| 7,13 | 5 | - | - | - | 1 | 3 | 7 | 15 |
| 2,19 | 5 | - | - | - | 1 | 3 | 7 | 15 |
| 2,25 | 5 | - | - | - | 1 | 3 | 7 | 15 |
| 2,31 | 5 | - | - | - | 1 | 3 | 7 | 15 |
| 3,19 | 5 | - | - | - | 1 | 3 | 7 | 15 |
| 3,25 | 5 | - | - | - | 1 | 3 | 7 | 15 |
| 3,31 | 5 | - | - | - | 1 | 3 | 7 | 15 |
| 2,37 | 6 | - | - | - | - | 1 | 3 | 7 |
| 2,41 | 6 | - | - | - | - | 1 | 3 | 7 |
| 2,47 | 6 | - | - | - | - | 1 | 3 | 7 |
| 2,55 | 6 | - | - | - | - | 1 | 3 | 7 |
| 2,59 | 6 | - | - | - | - | 1 | 3 | 7 |
| 2,61 | 6 | - | - | - | - | 1 | 3 | 7 |
| 3,37 | 6 | - | - | - | - | 1 | 3 | 7 |
| 3,41 | 6 | - | - | - | - | 1 | 3 | 7 |
| 3,47 | 6 | - | - | - | - | 1 | 3 | 7 |
| 3,55 | 6 | - | - | - | - | 1 | 3 | 7 |
| 3,59 | 6 | - | - | - | - | 1 | 3 | 7 |
| 3,61 | 6 | - | - | - | - | 1 | 3 | 7 |
| 7,19 | 6 | - | - | - | - | 1 | 3 | 7 |
| 7,25 | 6 | - | - | - | - | 1 | 3 | 7 |
| 7,31 | 6 | - | - | - | - | 1 | 3 | 7 |
| 2,3,19 | 6 | - | - | - | - | 1 | 3 | 7 |
| 2,3,25 | 6 | - | - | - | - | 1 | 3 | 7 |
| 2,3,31 | 6 | - | - | - | - | 1 | 3 | 7 |

(c) Number of polynomials having repeated common factors.

| Polynomial Order | Total No. of Polyn. | Prime factor polynomials and their order | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | 2:1 | 3:1 | 7:2 | 11:3 | 13:3 | 19:4 | 25:4 | 31:4 |
| 2 | 7 | 2 | 2 | 1 | . | . | . | . | . |
| 3 | 15 | 3 | 3 | 1 | 1 | 1 | . | . | . |
| 4 | 31 | 4 | 4 | 2 | 1 | 1 | 1 | 1 | 1 |
| 5 | 63 | 5 | 5 | 2 | 1 | 1 | 1 | 1 | 1 |
| 6 | 127 | 6 | 6 | 3 | 2 | 2 | 1 | 1 | 1 |
| 7 | 255 | 7 | 7 | 3 | 2 | 2 | 1 | 1 | 1 |
| 8 | 511 | 8 | 8 | 4 | 2 | 2 | 2 | 2 | 2 |

## 4. CONCLUSION

We have presented a simple and easy to implement algorithm to factorize a given polynomial with coefficients in GF(2). This algorithm can be used recursively to generate a table of prime polynomials in GF($2^m$). Some interesting properties of prime polynomials are deduced.

## REFERENCES


[1] W.W. Peterson and E.J. Weldon, *Error Correcting Codes*, MIT Press Cambridge, MA, 1972.

[2] E.R.Berlekamp, *Algebraic Coding Theory*, Mc-Graw Hill, NY, 1968.

[3] F.J. MacWilliams and N.J.A. Sloan, *The Theory of Error-Correcting, Codes*, North Holland, NY, 1977.

[4] D.E.R. Denning, Cryptography and Data Security, Addison-Wesley, Reading MA, 1983.

[5] C.S. Yeh, I.S. Reed and T.K.Truong, "Systolic multipliers for, Finite Fields GF($2^m$)", IEEE Trans. Comput., Vol. C-33, pp. 357-360, April 1984.

[6] S. Lin and D.J. Costello, *Error Control Coding*, Prentice Hall, New Jersey, 1983.

[7] A.M. Michelson and A.H. Levesque, *Error Control Techniques for Digital Communication*, John Wiley and Sons, NY, 1985.