Division Algorithm to search for monic irreducible polynomials over extended Galois Field GF(p^q).

Sankhanil Dey[1], Amlan Chakrabarti[2] and Ranjan Ghosh[3],
Department of Radio Physics and Electronics, University of Calcutta,
92 A P C Road, Kolkata-700009[1,3].
and
A K Choudhury School of Information Technology, University of Calcutta,
Sector-III, JD-2 block, Salt Lake City, Kolkata-700098[2].

Abstract. In modern era of computer science there are many applications of the polynomials over finite fields especially of the polynomials over extended Galois fields GF(p^q) where p is the prime modulus and q is the extension of the said Galois field, in the generation of the modern algorithms in the computer science, the soft computation, the cryptology and the cryptanalysis and especially in generation of the S-boxes of the cryptographic block and stream ciphers. The procedure and the algorithms of the subtraction and the division of the two Galois field polynomials over the Galois field GF(p^q) was remained untouched to the researchers of the applications of finite field theory in the computer science. In this paper the procedure and algorithms to subtract and divide the two Galois field polynomials over Galois field GF(p^q) or the two Galois field numbers over the Galois field GF(p^q) are introduced in detail. If a monic basic polynomial over the Galois field GF(p^q) (BP) [1] is divisible by any of the monic elemental polynomials over the Galois field GF(p^q) (EP) [1] except the constant polynomials (CPs) [1] over the Galois field GF(p^q) then the monic BP over the Galois field GF(p^q) is termed as the monic reducible polynomial (RP) [1] over the Galois field GF(p^q) and if a monic BP over the Galois field GF(p^q) is not divisible to any of the EPs over the Galois field GF(p^q) except the CPs over the Galois field GF(p^q) or more specifically to any monic EP over the Galois field GF(p^q) with half of the degree of the concerned monic BP over the Galois field GF(p^q) then the monic BP over Galois field GF(p^q) is called as the irreducible polynomial (IP) [1] over the Galois field GF(p^q). Here the common algorithm to generate all the monic IPs over the Galois field GF(p^q) is introduced. The time complexity analyses of the algorithms prove the said algorithms to be less time consuming and efficient.

1. Introduction and Scope. The polynomials over the finite fields especially the polynomials over the extended Galois field GF(p^q) where p is the prime modulus and q is the extension of the said Galois field, have many important applications in computer science such as generation of 4-bit and 8-bit S-boxes of cryptographic block ciphers [1][2]. Specially irreducible polynomials (IPs) over the Galois field GF(p^q) play such an important role [3]. Generation of the monic IPs over the Galois field GF(p^q) for large values of p and q is the unbroken stone in this research scenario. To break this stone it is needed to generate the procedures and the algorithms for the subtraction, the multiplication and the division of the two Galois field polynomials over the same Galois field GF(p^q). A small review of the relevant articles on generation of IPs over the Galois field GF(p^q) is made in section 2.

To subtract two Galois field polynomials over the Galois field GF(p^q) generate the GFNs [1] of the two said polynomials and subtract each corresponding digit of the GFN with small decimal equivalent (DE) from the GFN with large DE and modulate the result with p to obtain the corresponding subtracted digit. If the subtracted digit is negative then add p as borrow to the next position GFN with small decimal equivalent (DE). If two GFNs have unequal numbers of digits then pad the GFN with small decimal equivalent (DE) with 0s in left. A brief description of the procedure of the subtraction of the two Galois field polynomials over the Galois field GF(p^q) and the algorithm for the procedure is detailed in section 3.2.

To divide two Galois field polynomials over the Galois field GF(p^q) generate the GFNs [1] of the two said polynomials at first. Division over the Galois field GF(p^q) procedure is same as decimal division but there are some important modifications in this division procedure. The product of divisor and each digit of quotient is subtracted from the same number of digits from most significant bit of the dividend to obtain the residue and the subtraction is

made by the procedure defined in section 3.2. The total division procedure and algorithm two Galois field polynomials over the Galois field GF(p^q) is described in sec 3.3.

Now to generate the DEs of all the monic IPs over the Galois field GF(p^q) each monic BP over the Galois field GF(p^q) is checked for positive residues for divisions over the Galois field GF(p^q) with all the monic EPs except CPs over the Galois field GF(p^q) with degree $\leq$ q/2. If residues are positive for all the divisions over the Galois field GF(p^q) for the monic BP over the Galois field GF(p^q) then the monic BP over the Galois field GF(p^q) is termed as IPs. The detail procedure and the detail algorithm for the BPs over the Galois field GF(2^4) are given in section 4.1 and section 4.2 respectively. The detail algorithm for the BPs over the Galois field GF(p^q) is given in section 4.3 and the comparison of the time complexities of the multiplication, division and Rabin's algorithm are given in section 4.4 to prove the said algorithm to be the best.

The conclusion and acknowledgement of the paper is given in section 5 and section 6 respectively.

2. Review work. Short reviews on relevant and related articles are made in this section.

- **Rudolf Church [1935][4].** Here two monic EPs over the Galois field GF(p^q) are multiplied by paper pen to generate all monic RPs over the Galois field GF(p^q). All monic RPs over the Galois field GF(p^q) are cancelled out from the list of the monic BPs over the Galois field GF(p^q) to extract all monic IPs over the Galois field GF(p^q). Here the value of p varies from 2 [q=2 to q=11] to 7 [q=2 to q=4].
- **Zaman et. al [2014][5].** Here two monic EPs over the Galois field GF(p^q) are multiplied and then divided by all monic BPs over the Galois field GF(p^q) by matrix method. If for any division the residue is 1 then the two monic EPs over the Galois field GF(p^q) are multiplicative inverses (MIs) of each other.
- **Dey and Ghosh [2017-a][6].** Here the procedure to multiply of GFNs of two polynomials over the Galois field GF(p^q) is illustrated. The each digit of a GFN or the coefficients of each degree term of the polynomial over the Galois field GF(p^q) are multiplied to all digits of other GFN consecutively. Then the obtained digits or coefficients with same degree terms are added and modulated with p to obtain the resultant GFN or the coefficients of the resultant polynomial over the Galois field GF(p^q).
- **Dey and Ghosh [2017-b][7].** In this algorithm the decimal equivalents of each of two monic EPs over the Galois field GF(p^q) at a time with highest degree d and (q-d) where d **€** {0,..,(q-1)/2} , have been split into the p-nary coefficients of each term of two said monic EPs over the Galois field GF(p^q). The coefficients of each term in each two Monic EPs or two GFNs are multiplied, added respectively with each other and modulated to obtain the p-nary coefficients of each term of the RPs over the Galois field GF(p^q). The DE of the resultant monic BP over the Galois field GF(p^q) is termed as the DE of an RP over the Galois field GF(p^q). The DE of BPs over the Galois field GF(p^q) belonging to the list of RPs over the Galois field GF(p^q) have been cancelled leaving behind the monic IPs over the Galois field GF(p^q).

3. Procedure and Algorithm of subtraction and division over the Galois field GF(p^q).

The algorithms of subtraction, multiplication, division of the two GFNs [1] or polynomials over the Galois field GF(p^q) is remained untouched by computer science community. The generation of the GFNs is described in subsection 3.1. The procedure to obtain the difference of two GFNs over the Galois field GF(p^q) or subtraction of the two GFNs over the Galois field GF(p^q) is described in subsection 3.2 and division of the two GFNs over the Galois field GF(p^q) is described in subsection 3.3.

3.1 Galois Field Numbers or GFNs. Coefficient of each degree term of a polynomial are arranged sequentially from highest to lowest degree in a decreasing sequence of degree terms (Coefficient of highest degree term is in MSB and coefficient of lowest degree term is in LSB) to obtain Galois Field Numbers (GFNs) for polynomials over the Galois fields GF(p^q) where p is the prime modulus and q is the extension of the said Galois field. There are two special types of GFNs. Binary Coded Numbers or BCN for polynomials over the Galois field GF(2^q) and Finite Field Numbers (FFNs) for polynomials over finite field GF(p^q) where p is non-prime. Examples of some GFNs, BCNs and FFNs are given in table.1, table.2 and table.3 respectively below and the description of the said tables are also given below.

Row	DEs	Polynomials	BCNs
Col→	**1**	**2**	**3**
1	14406	$6x^4$	60000
2	14407	$6x^4+1$	60001
3	2443	x^4+6x	10060
4	2414	x^4+x+6	10016

Table.1. GFNs of four Galois field polynomials over the Galois field GF(7^4).

Row	DEs	Polynomials	BCNs
Col→	**1**	**2**	**3**
1	16	x^4	10000
2	17	x^4+1	10001
3	18	x^4+x	10010
4	19	x^4+x+1	10011
5	20	x^4+x^2	10100
6	21	x^4+x^2+1	10101
7	22	x^4+x^2+x	10110
8	23	x^4+x^2+x+1	10111
9	24	x^4+x^3	11000
A	25	x^4+x^3+1	11001
B	26	x^4+x^3+x	11010
C	27	x^4+x^3+x+1	11011
D	28	$x^4+x^3+x^2$	11100
E	29	$x^4+x^3+x^2+1$	11101
F	30	$x^4+x^3+x^2+x$	11110
G	31	$x^4+x^3+x^2+x+1$	11111

Table.2. BCNs of 16 Galois field polynomials over the Galois field GF(2^4).

Row	DEs	Polynomials	BCNs
Col→	**1**	**2**	**3**
1	768	$3x^4$	30000
2	770	$3x^4+2$	30002
3	264	x^4+2x	10020
4	267	x^4+2x+3	10023

Table.3. FFNs of four Galois field polynomials over the Galois field GF(4^4).

Description of Table.1, Table.2, and Table.3:

Table.1: Examples of four GFNs over the Galois field GF(7^4) are given in row 1 through 4 of Table.1. DEs of the polynomials, the polynomials itself and the respective GFNs are given in column 1, 2 and 3 of the respective rows.

Table.2: Examples of four BCNs over the Galois field GF(2^4) are given in row 1 through 16 of Table.2. DEs of the polynomials, the polynomials itself and the respective BCNs are given in column 1, 2 and 3 of the respective rows.

Table.3: Examples of four FFNs over the Galois field GF(4^4) are given in row 1 through 4 of Table.3. DEs of the polynomials, the polynomials itself and the respective FFNs are given in column 1, 2 and 3 of the respective rows.

3.2 Procedure and Algorithm of Subtraction of two GFNs:

To subtract two Galois field polynomials over the Galois field GF(p^q) generate the GFNs [1] of the two said polynomials and subtract each corresponding digit of the GFN with small decimal equivalent (DE) from the GFN with large DE and modulate the result with p to obtain the corresponding subtracted digit. If the subtracted digit is negative then add p as borrow to the next position GFN with small decimal equivalent (DE) and modulate with p. If two GFNs have unequal numbers of digits then pad the GFN with small decimal equivalent (DE) with 0s in left. A brief description of the procedure of the subtraction of the two Galois field polynomials over the Galois field GF(p^q) is given in subsection 3.2.1 and the algorithm for the procedure is detailed in section 3.2.2.

3.2.1 Procedure:

To subtract two Galois field polynomials over the Galois field GF(p^q) generate the GFNs [1] of the two said polynomials and subtract each corresponding digit of the GFN with small decimal equivalent (DE) from the GFN with large DE and modulate the result with p to obtain the corresponding subtracted digit. If the subtracted digit is negative then add p as borrow to the next position GFN with small decimal equivalent (DE) and modulate with p. If two GFNs have unequal numbers of digits then pad the GFN with small decimal equivalent (DE) with 0s in left. Example for two BCNs and two GFNs are given below,

Key Definitions.

Basic polynomials (BPs) over Galois field GF(2^4). Polynomials over the Galois field GF(2^4) with highest degree 4 are termed as BPs over Galois field GF(2^4).

Elemental polynomials (EPs) over Galois field GF(2^4). Polynomials over Galois field GF(2^4) with highest degree less than 4 are termed as EPs over Galois field GF(2^4).

Binary Coded Numbers (BCNs) or Galois field Numbers (GFNs) over Galois field GF(2^4). If it is considered that coefficient of highest degree term of the concerned polynomial is the MSB of the number and coefficient of lowest degree term of the concerned polynomial is the LSB of the number and other coefficients of highest degree to lowest degree term are arranged sequentially from MSB to LSB in the number then the number constructed with coefficients of the concerned polynomial is termed as BCN or which is also a GFN over Galois field GF(2^4).

Subtraction of two BCNs over Galois field GF(2^4):

Two EPs over Galois field GF(2^4) are,

EPs	BCNs or GFNs
x	0010
x^3+1	1001

Now,

BCN(x) < BCN(x^3+1). If we subtract BCN(x) from BCN(x^3+1) we get, subtract in decimal each digit of BCN(x) from BCN(x^3+1) and modulate the result with 2 when result is negative add borrow 1 to next position of the BCN(x) and modulate with 2.

A. **1-0-0-1**

B. **0-0-1-0**

Difference. 0-1-1-1

3.2.2 Algorithm:

The algorithm is given below,

Start.

Step 1: The four bits of the 1st BCN or BCN(x^3+1) with greater value of DE are stored at bcn_large.bit0, bcn_large.bit1, bcn_large.bit2, bcn_large.bit3 from MSB to LSB respectively and The four bits of the 2nd BCN or BCN(x) with smaller value of DE are stored at bcn_small.bit0, bcn_small.bit1, bcn_small.bit2, bcn_small.bit3 from MSB to LSB respectively.

Step 2: The subtraction is started from LSB.

Step 3: bcn_small.bit3 is subtracted from bcn_large.bit3 and the obtained digit is modulated with 2. If the result is negative then add borrow 1 to the bcn_small.bit2 and subtract it from bcn_large.bit2 and modulate the obtained digit with 2 to obtain the 2nd subtracted digit of the difference. The procedure is going on till the subtraction of bcn_small.bit0 from bcn_large.bit0.

Step 4: The obtained four corresponding digits are stored in diff.bit0, diff.bit1, diff.bit2 and diff.bit3 respectively.

Stop.

3.3 Procedure and Algorithm of Division of two GFNs:

To divide two Galois field polynomials over the Galois field GF(p^q) generate the GFNs [1] of the two said polynomials at first. Division over the Galois field GF(p^q) procedure is same as decimal division but there are some important modifications in this division procedure. The product of divisor and each digit of quotient are subtracted from the same number of digits from most significant bit of the dividend to obtain the residue and the subtraction is made by the procedure defined in section 3.2. The total division procedure is given in subsection 3.3.1 and the algorithm to divide two Galois field polynomials over the Galois field GF(p^q) is described in subsection 3.3.2.

3.3.1 Procedure.

In division of the two Galois field polynomials over the Galois field GF(p^q) generate the GFNs [1] of the two said polynomials at first. Division over the Galois field GF(p^q) procedure is same as decimal division but there are some important modifications in this division procedure. The product of divisor and each digit of quotient are subtracted from the same number of digits from most significant bit of the dividend to obtain the residue and the subtraction is made by the procedure defined in section 3.2. The procedure for the two GFNs more specifically for the two BCNs is as follows,

Two Polynomials over the Galois field GF(2^4) are,

Polynomials	BCNs or GFNs
x	0010
x^3+1	1001

Now,

BCN(x) < BCN(x^3+1). The division of the BCN(x^3+1) by BCN(x) would result as follows,

```
10)1001(100
   10
  ----
   000
    00
  ----
    01
    00
  ----
     1
```

In this division the division is similar to decimal division but the subtraction is according to subtraction of two BCNs over Galois field GF(2^4).

3.3.2 Algorithm.

The algorithm for the division of the two BCNs over the Galois field GF(2^4) is given below,

Start.

Step 0. Let us take the DEs of the two polynomials A and B over Galois field GF(2^4).

Step 1. Convert the two numbers into two BCNs, BCN(A) and BCN(B).

Step 2. If **(**BCN(A)>BCN(B) then [avoid zero padding],

Step 3. divide BCN(A) by BCN(B) with decimal division to obtain quotient D(A/B) and residue R(A/B) but the only difference is the subtraction used in division is according to subtraction of two BCNs over Galois field GF(2^4).

Stop.

4. Procedure and Algorithm to Generate all the monic IPs over the Galois field GF(2^4) and the Galois field GF(p^q).

The procedure to generate all the monic IPs over the Galois field GF(2^4) is described in subsection 4.1. The algorithm for the said procedure for the IPs over the Galois field GF(2^4) is given in subsection 4.2. Finally the algorithm for the said procedure for the IPs over the Galois field GF(p^q) is given in subsection 4.3.

4.1 Procedure.

Now to generate the DEs of all the monic IPs over the Galois field GF(p^q) each monic BP over the Galois field GF(2^4) is checked for positive residues for divisions over the Galois field GF(p^q) with all the monic EPs except CPs over the Galois field GF(p^q) with degree $\leq$ q/2. If residues are positive for all the divisions or incomplete division for all the time over the Galois field GF(p^q) for the monic BP over the Galois field GF(p^q) then the monic BP over the Galois field GF(p^q) is termed as IPs.

4.2 Algorithm to generate all the monic IPs over the Galois field GF(2^4).

The Algorithm over the Galois field GF(2^4) for the procedure given in subsection 4.1 is given below,

Start.

Step 1. Take the DEs of all the monic BPs one by one i.e. 16 to 31 one by one.

Step 2. Convert each DE to its BCN over the Galois field GF(2^4).

Step 3. Divide each monic BP with BCNs over the Galois field GF(2^4) of the all monic EPs from 2 to 7 (2^1 to 2^{3-1}) but the division is according to the procedure given in section 3.1.

Step 4. If for a particular monic BP all the divisions are incomplete or there is a residue. Then the BP is termed as the monic IP otherwise monic RP.

Stop.

4.3 Algorithm to generate all the monic IPs over the Galois field GF(p^q).

The algorithm over the Galois field GF(p^q) for the procedure given in subsection 4.1 is given below,

Start.

Step 1. Take the DEs of all the monic BPs one by one i.e. p^q to p^{q+1}-1 one by one.

Step 2. Convert each DE to its BCN over the Galois field GF(p^q).

Step 3. Divide each monic BP with BCNs over the Galois field GF(p^q) of the all monic EPs from (p^1 to p^{q-1}-1) but the division is according to the procedure given in section 3.1.

Step 4. If for a particular monic BP all the divisions are incomplete or there is a residue. Then the BP is termed as the monic IP otherwise monic RP.

Stop.

4.4 Comparison of time complexity of the given algorithm with Rabin's Algorithms.

The new division algorithm to find the monic IPs over Galois field GF(p^q) have a time complexity of O(n^2). Since time complexity of Rabin's algorithm and its modification depends upon the value of prime modulus p so it becomes slower for large value of p. Now in this algorithm the complexity depends upon the value of extension q so they are faster and eligible to find monic IPs for very large value of p as well as extension q.

Algorithms	Division Algorithm	Rabin's Algorithm	Rabin's Algorithm(mod)
Time Complexity	$O(n^2)$	$O(n^4(\log P)^3)$	$0(n^4(\log p)^2 + n^3(\log P)^3)$

Table.4. Comparison of Time Complexity of the division algorithm with Rabin's and Modified Rabin's Algorithm.

5. **Conclusion.** From the last few decades computer scientists try to break the untouched stone of division algorithm to reduce the time complexity of many algorithms in computer science and artificial intelligence. In this paper this stone is broken to find the large numbers of monic IPs over the extended Galois field $GF(p^q)$ where prime modulus p is very large with a very large value of extension q. The algorithm reduces the required time almost 100 times rather than the previous algorithms and the excellence of the algorithm is also increased for 100 times than the previous ones. The time complexity analysis proves the previous statements true and the division algorithm to be the best algorithm ever to find the large numbers of monic IPs over the extended Galois field $GF(p^q)$ where prime modulus p is very large with a very large value of extension q.

6. **Acknowledgements.** I would like to acknowledge Prof. (Dr.) Gopa Sen, Head Dept. Radio Physics and Electronics of the University of Calcutta and Prof. Amlan Chakrabarti, Director of the A K Choudhury School of Information Technology of the University of Calcutta for providing me the uninterrupted infrastructure to carry out the research. I would also like to thank TEQIP-Phase-II for providing me the financial support up to 30th November 2016.

References.

1. Sankhanil Dey, Amlan Chakrabarti , Ranjan Ghosh . (2019) 4-bit crypto S-boxes: Generation with irreducible polynomials over Galois field GF(2^4) and cryptanalysis., International Journal of Tomography and Simulation, ISSN: 2319-3336, Vol. 32, Issue No. 3, CESER publication.

2. Sankhanil Dey and Ranjan Ghosh (2018)"A smart review and two new techniques using 4-bit Boolean functions for cryptanalysis of 4-bit crypto S-boxes.", Vol.40, issue.3, pp.1-19, International Journal of Computers and Applications, Taylor and Francis publishers, ISSN. 1206-212X. DOI. **https://doi.org/10.1080/1206212X.2018.1504459**.

3. Joan Daemen,Vincent Rijmen (2000), AES Proposal: Rijndael,http://csrc.nist.gov/encryption/aes/ Last Visited: 7th February 2001.

4. Church R, Tables of irreducible polynomials for the first four prime moduli, The Annals of Maths., 2nd Series, vol. 36, no. 1, 198-209, Jan (1935) http://www.jstor.org/stable/1968675.

5. JKM Sadique Uz Zaman, Sankhanil Dey, Ranjan Ghosh, (2015) An Algorithm to find the Irreducible Polynomials over Galois Field GF(p^m), International Journal of Computer Applications 109(15):24-29, DOI:10.5120/19266-1012.

6. Sankhanil Dey and Ranjan Ghosh, (2017) A new mathematical method to search irreducible polynomials using decimal equivalents of polynomials over Galois field $GF(p^q)$, Journal: Circulation in Computer Science, Vol.2, No.11. pp-17-22, CSL Press, New York, DOI, ISSN. 2456-3692. **https://doi.org/10.22632/ccs-2017-252-68**.

7. Sankhanil Dey. and Ranjan Ghosh. (2018) Search for Monic Irreducible Polynomials with Decimal Equivalents of Polynomials over Galois Field $GF(p^q)$. Open Journal of Discrete Mathematics, Scientific Research Publishers, 8 (1), 21-33, ISSN online. 2161-7643 ISSN online. 2161-7635. **https://doi.org/10.4236/ojdm.2018.81003**.