# Multiplication over Extended Galois Field: A New Approach to Find Monic Irreducible Polynomials over Galois Field GF($p^q$).

Sankhanil Dey[1] and Ranjan Ghosh[2],
sdrpe_rs@caluniv.ac.in[1], rghosh47@yahoo.co.in[2],
Institute of Radio Physics and Electronics,
University of Calcutta.

**Abstract.** Searching for Monic Irreducible Polynomials (IPs) over extended Galois Field GF($p^q$) for large value of prime moduli p and extension to Galois Field q is a well needed solution in the field of Cryptography. In this paper a new algorithm to obtain Monic IPs over extended Galois Fields GF($p^q$) for large value of p and q has been introduced. The algorithm has been based on Multiplication algorithm over Galois Field GF($p^q$).Time complexity analysis of the said algorithm has also been executed that ensures the algorithm to be less time consuming.

**1. Introduction**: The Basic Polynomials or BPs over Galois field GF($p^q$) have been polynomials with highest degree of terms d equal to Galois field Extensions q (d =q) and so it must have (q+1) terms . Elemental Polynomials or EPs have been polynomials with highest degree of terms d less than Galois field Extensions q (d <q) and so it must have less than (q+1) terms from 1 through q. BPs with leading co-efficient unity have been termed as Monic BPs. Monic BPs that do not have two Monic EPs rather than Constant Polynomials have been termed as Monic IPs. The EPs with degree d = 0 has been termed as Constant Polynomials (CPs)and they are p in numbers and not in consideration in this paper. Generator Polynomials or GPs have been polynomials with number of terms less than or equal to (q+1) and the code word or generated polynomials from BPs have been divisible by GPs but that are also not in consideration in this paper.

There are many algorithms in past that were introduced to find Monic IPs over Galois Fields GF(p) and Extended Galois Fields GF($p^q$) for small values of Prime Modulii p as well as small values of extension q. The hands on computation to find Monic Irreducible Polynomials over Galois Field GF($p^q$) for p = 2, q = 2 through 11, p = 3, q = 2 through 7, p = 5, q = 2 through 5 and for p = 7, q = 2 through 4 has initiated by Church [1] in his contribution. The GF equivalents of each Monic Basic Polynomial (BP) for p = 2 through 7 had also been reported in his contribution [1]. In his contribution each two Monic Elemental Polynomials (Eps) have been multiplied to obtain the reducible Monic BPs. The search for Monic IPs ended up with cancellation of all reducible Monic BPs leaving behind the Irreducible Monic BPs. In Rabin's Algorithm [2] all Monic BPs (F(x)) over Galois Field GF(p) of degree n has been tested for divisibility with ($x^n$-x) and the gcd of (F(x), $x^{nki}$-x) where the $k_i$ have been all prime divisors of n , to be unity. If any monic BP, F(x) satisfies both condition, the Monic BP is termed as IP. According to Zaman and Ghosh [3] if the residue of each polynomial division of each Monic BP with all EPs are unity or every EP has a multiplicative inverse over Galois Field under a Monic BP then the Monic BP is termed as a Monic IP. The algorithm is also implemented using Galois Field division and termed as composite algorithm [3].

A basic polynomial BP(x) over finite field or Galois Field GF($p^q$) has been expressed as,

$$BP(x) = a_q x^q + a_{q-1}x^{q-1} + - - - + a_1x + a_{0.}$$

B(x) has (q+1) terms, where $a_q$ is non-zero and has been termed as the leading coefficient [4]. A polynomial has been termed as Monic if $a_q$ is unity, else it is Non-Monic. The GF($p^q$) have ($p^q$ – p) EPs or ep(x) in a range from p to ($p^q$ -1) each of whose representation involves q terms with leading coefficient $a_{q–1}$. The expression of ep(x) is written as,

$$ep(x) = a_{q-1}x^{q-1} + - - - + a_1x + a_0 \text{ , where } a_1 \text{ to } a_{q-1} \text{ are not simultaneously zero.}$$

BP(x) with ep(x) as a factor except Constant Polynomials GF($p^q$), Have been termed as Reducible Polynomials (RPs). BP(x) with factors itself and Constant Polynomials or no EPs as a factor has been termed as IPs or IP(x) [5] and is expressed as,

$$IP(x) = a_q x^q + a_{q-1}x^{q-1} + - - - + a_1x + a_0 \text{ , where } a_q \neq 0.$$

PeerJ Preprints | https://doi.org/10.7287/peerj.preprints.3258v1 | CC BY 4.0 Open Access | rec: 17 Sep 2017, publ: 17 Sep 2017

In Galois field GF($p^q$), the Decimal Equivalents (DEs) of BPs with extension q vary from $p^q$ to ($p^{q+1}$ - 1) while for EPs, DEs vary from p to ($p^q$ – 1). Some of Monic BPs has been considered as IPs, since IPs have no Monic EPs as a factor except Constant Polynomials.

In this algorithm EPs with degree d and q-d where d<q for d = 1,2,…,(q-1)/2 have been multiplied over Galois Field GF($p^q$) through Multiplication Algorithm to ensure the factorization or reducibility of the product Monic BPs. The Left alone BPs or that do not have any factor except CPs have been termed as Monic IPs.

In this paper for clarity understanding, the proposed algorithm has been presented in Sec.2 for Galois Field GF($p^q$) and the algorithm has been described with the example of Galois Field GF($7^7$), where p=7 and q=7 in the same section . Sec. 3 demonstrates the obtained results to show that the proposed searching algorithm is actually able to search over any Galois field GF($p^q$) with any value of prime modulus and its extension, such as, p €{ 3, 5, 7,....,101,..,p} and q € { 2, 3, 5, 7,…,101,….q}. In Sec.4 and 5, the conclusion references have been illustrated.

## 2. Algorithm to find Monic of IPs over Galois Field GF($p^q$).

In this section the new algorithm to search for DEs of all Monic IPs over Galois Field GF($p^q$) has been described with example of GF($7^7$), where p=7 and q=7. The detailed structural description of the algorithm has given in sub sec.2.1. The detailed mathematical description of the algorithm has been described in sub sec.2.2. The Computational Algorithm is demonstrated in sec.2.3.The example of the said algorithm for Galois Field GF($7^7$), where p=7 and q=7 is given in sub sec 2.4. The Time complexity analysis has been described in sub sec.2.5.

### 2.1. Structural Description of the Algorithm.

In this algorithm the decimal equivalents of each of two Monic EPs 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 those two Monic EPs. The coefficients of each term in each two Monic EPs are multiplied, added respectively with each other and modulated to obtain the p-nary coefficients of each term of the Monic BP. The DE of the resultant Monic BP is termed as the DE of a reducible Monic BP. The DE of BPs belonging to the list of reducible polynomials are cancelled leaving behind the Monic IPs. For Galois Field GF($p^q$), where p is the prime modulus and q is the extension of the field, the algorithm is given as follows,

**Start.**
**Step 1.** Generate DEs of all Monic EPs Dec(ep(x)) over Galois Field GF($p^q$).
**Step 2.** Split Dec(ep($x_1$)), Dec(ep($x_2$)) with highest degree d and (q-d) respectively where d **€** {0,..,(q-1)/2}, are split into p-nary coefficients or each term of those two each Monic EPs ep($x_1$) and ep($x_2$).
**Step 3.** Multiply and add terms with degree d **€** {d,d-1,.., 0} and (q-d) **€** {q-d,q-d-1,.., 0} to obtain the decimal coefficients of each degree terms of the Monic BP, BP(x).
**Step 4.** convert Decimal Coefficient of each term of Monic BP, BP(x) into p-nary coefficients.
**Step 5.** Obtain the DE of the Monic BP, BP(x) or Dec(BP(x)) as the DE of a Reducible Polynomial or RP.
**Step 6.** The DEs of Monic BPs belonging to the list of Monic RPs are cancelled leaving behind the Monic IPs.
**Stop.**

### 2.2 Mathematical Structure of the Algorithm.

Here it has been intend to find the Monic IPs over Galois Field GF($p^q$), where p is the prime modulus and q is the extension of the prime modulus and p must be a prime integer. Since the indices of multiplicand and multiplier are added to obtain the product., the extension q can be demonstrated as a sum of two integers, $d_1$ and $d_2$, The degree of highest degree term present in EPs of GF($p^q$) is (q-1) to 1, since the polynomials with highest degree term 0, are CPs and they do not play any significant role here, so they are neglected. Hence the two set of Monic EPs for which the multiplication is a Monic BP, have the degree of highest degree terms $d_1$, $d_2$ where, $d_1$ € {1,2,3,..,((q-1)/2)}, and the corresponding values of $d_2$ € {(q-1), (q-2), (q-3).,...,q-((q-1)/2)}. Number of coefficients in the Monic BPs, BP(x) = (q+1); they are defined as $BP_{0,}$ $BP_{1,}$ $BP_{2,}$ $BP_{3,}$ $BP_{4,}$ $BP_{5,}$ $BP_{6,}$ $BP_{7,\ldots\ldots,}$ $BP_{q,}$ where the value of suffix also indicates the degree of the term of the obtained Monic BP. For Monic polynomials $BP_q$= 1.

Coefficients of each term in the 1st Monic EP $EP^0$, where, $d_1$ € {1,2,…..,((q-1)/2)}; are defined as $EP_0^{0}$, $EP_1^{0}$,……., $EP_{((q-1)/2-1)}^{0}$. Coefficients of each term in the 2nd Monic EP, $EP^1$ where $d_2$ € {(q-1), (q-2), (q-3).,...,q-((q-1)/2-1)}; are defined as $EP_0^{1}$, $EP_1^{1}$, $EP_2^{1}$, $EP_3^{1}$, $EP_4^{1}$, … , $EP_{q-((q-1)/2-1)}^{1}$. The value in suffix also gives the degree of the term of the Monic EPs. Total number of blocks is the number of integers in $d_1$ or $d_{2,}$ i.e. (q-1)/2 .

Now, the Mathematical Structure of (q-1)/2th block for the algorithm has been given as follows,

**(q-1)/2th block:**

$$\mathbf{BP_0} = (EP_0^{\,0} \times EP_0^{\,1}) \bmod p.$$
$$\mathbf{BP_1} = (EP_0^{\,0} \times EP_1^{\,1} + EP_1^{\,0} \times EP_0^{\,1}) \bmod p.$$
$$\mathbf{BP_2} = (EP_0^{\,0} \times EP_2^{\,1} + EP_1^{\,0} \times EP_1^{\,1} + EP_2^{\,0} \times EP_0^{\,1}) \bmod p.$$
$$\mathbf{BP_3} = (EP_0^{\,0} \times EP_3^{\,1} + EP_1^{\,0} \times EP_2^{\,1} + EP_2^{\,0} \times EP_1^{\,1} + EP_3^{\,0} \times EP_0^{\,1}) \bmod p.$$

……………………………………………………………………

……………………………………………………………………

$$\mathbf{BP_{q-1}} = (EP_0^{\,0} \times EP_{(q-1)}^{\,1} + EP_1^{\,0} * EP_{(q-2)}^{\,1} + \ldots\ldots\ldots\ldots + EP_{(q/2-1)}^{\,0} * EP_{(q-1)-(q-1)/2}^{\,1}) \bmod p.$$
$$\mathbf{BP_q} = (EP_{(q-1)/2}^{\,0} * EP_{q-(q-1)/2}^{\,1}) \bmod p.$$

Now the given Monic BP has been illustrated in Eq.1. and its DE of Monic BP has been calculated as in eq.2,

$$\mathbf{BP(x)} = BP_q\,x^q + BP_{q-1}\,x^{q-1} + \ldots. + BP_5\,x^5 + BP_4\,x^4 + BP_3\,x^3 + BP_2\,x^2 + BP_1\,x^1 + BP_0\,x^0 \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots..(1)$$
$$\mathbf{Decm\_eqv(BP(x))} = BP_q \times p^q + BP_{q-1} \times p^{q-1} + \ldots. + BP_5 \times p^5 + BP_4 \times p^4 + BP_3 \times p^3 + BP \times p^2 + BP_1 \times p^1 + BP_0 \times p^0 \ldots\ldots(2)$$

Similarly DEs of all resultant Monic BPs or RPs for all have been calculated. The Monic BPs belonging to the list of RPs are cancelled leaving behind the desirable IPs.

### 2.3. Description of the Computational Algorithm.

Here the Monic BPs over Galois Field GF($p^q$) has been presented as BP(x) and EPs over the same Galois field is presented as ep(x). For Galois Field GF($p^q$) the prime modulus € p and the extension of the prime modulus € q. Highest degree term of the 1st EP, ep($x_1$) is $d_1$ € {1,2,3,…………,(q-1)/2} and second EP, ep($x_2$) is $d_2$ € { (q-1), (q-2), (q-3),...,q-(q-1)/2}. Number of terms in 1st EP € {N($d_1$)} and number of terms in 2nd EP € {N($d_2$)}. Coefficients of each ep(x) are demonstrated as $EP_{ep\_indx\_i}$, where $1 \leq i \leq 2$.

Here Number of terms in Monic BP € q+1. Coefficients of BP(x) = $BP_{bp\_indx}$, where $0 \leq bp\_indx \leq q$, The said Computational Algorithm is as follows,

```
        Start
Step 1. For block € {1, 2, 3,…..,N($d_1$) or N($d_2$)} do the following steps. // Calculating Number of blocks need to calculate all monic RPs
Step 2. For ep_index_1 € {1, 2, 3,…, (q-1)/2} do the following steps. // Accessing each 1st Monic EPs
Step 3. For ep_index_2 € {(q-1), (q-2),….., q-((q-1)/2)} do the following steps. // Accessing each 2nd Monic EPs.
Step 4. For bp_index € {0, 1, 2,……,q} do the following steps. // Accessing each term of Monic BP.
Step 5. For $P_1$ € {2, 3,…,N($d_1$)} and $P_2$ € {(q-1)+1,(q-2)+1,…,N($d_2$)} do the following steps.//Accessing Each term of Monic EPs
Step 6. $BP_{bp\_indx} = (\Sigma(EP_{ep\_indx\_1}^{\,p1} \times EP_{ep\_indx\_2}^{\,p2})) \bmod p$;//calculating each coefficient of Monic BPs.
        End For; // End of For loop $P_1$ and $P_2$
        End For; // End of For loop bp_index
        End For; // End of For loop ep_index_2
        End For; // End of For loop ep_index_1
        End For; // End of For loop block
Stop.
```

### 2.4 Time Complexity of the New Algorithm.

This Algorithm have a time complexity of O($n^5$). Means it is much faster as Rabin's algorithm [7] for larger value of prime modulus and its modification [7]. Since the time complexity of the both Rabin's algorithm and its modification depends upon the value of prime modulus so it becomes a slow algorithm for large value of the prime modulus. But the new algorithm is much effective and works better as the value of prime modulus and the extension of prime modulus grows larger since time complexity depends only on the value of the extension of the Galois field. So this algorithm is suitable to find monic Irreducible polynomials of higher value of prime modulus and the extension of prime modulus .Comparison of time complexity of the new algorithm with other Algorithms is given below,

| Algorithms | New Algorithm | Rabin's Algorithm | Rabin's Algorithm(mod) |
|---|---|---|---|
| **Time Complexity** | $O(n^5)$ | $O(n^4(\log P)^3)$ | $0(n^4(\log p)^2 + n^3(\log P)^3)$ |

### 2.5. Description of the Computational Algorithm for Galois Field GF($7^7$).

Here the Basic polynomials over Galois Field over Galois Field GF($7^7$) is presented as BP(x) and Elemental polynomials over the same Galois field is presented as ep(x). For Galois Field GF($7^7$) the prime modulus = 7 and the extension of the prime modulus = 7. Highest degree term of the 1st elemental polynomial ep($x_1$) are $d_1$ € {1, 2, 3} and second elemental polynomial ep($x_2$) are $d_2$ **€ {**6, 5, 4}. Number of terms in 1st elemental polynomial: N($d_1$) **€ {**2,3,4} and number of terms in 2nd elemental polynomial: N($d_2$) **€ {**7,6,5} respectively. Coefficients of each ep(x) are demonstrated as EPep$_{\_indx\_i}$, where $1 \leq i \leq 2$.

Here Number of terms in Basic Polynomial = 8. Coefficients of BP(x) = BP$_{bp\_indx,}$ where $1 \leq$ bp_indx $\leq 8$, The said Computational Algorithm is as follows,

```
Step 1.  for block € {1,2,3} do the following steps.
Step 2.  for bp_index € {1,2,3,…, 8} do the following steps.
Step 3.  for ep_index_1 € {1,2,3} do the following steps.
Step 4.  for ep_index_2 € {6,5,4} do the following steps.
Step 5.  for $P_1$ € {2,3,4} and $P_2$ € {7,6,5} do the following steps.
Step 6.  $BP_{bp\_indx} = (\Sigma(EP_{ep\_indx\_1}^{p1} \times EP_{ep\_indx\_2}^{p2})) \bmod p$;
         End For; // End of For loop $P_{1 \text{ and}}$ $P_2$
         End For; // End of For loop bp_index
         End For; // End of For loop ep_index_2
         End For; // End of For loop ep_index_1
         End For; // End of For loop block

Step 7.  Stop.
```

## 3. Results.

The algebraic method or the above pseudo code has been tested on GF($3^3$),GF($7^3$),GF($11^3$), GF($101^3$), GF($3^5$), GF($7^5$), GF($3^7$), GF($7^7$),. Number of Monic IPs given by this algorithm are same as in hands on calculation by the theorem to count Monic IPs over Galois Field GF($p^q$) [1]. The list of Numbers of Monic IPs for a particular Galois Field is given below for all of the Eight Extended Galois Fields. The list of all Irreducible Monic BPs of Eight extended Galois fields are given as supplementary material.

| Ex.GF. | GF($3^3$) | GF($7^3$) | GF($11^3$) | GF($101^3$) |
|---|---|---|---|---|
| **Number of IPs.** | 8 | 112 | 440 | 343400 |
| **Ex.GF.** | **GF($3^5$)** | **GF($7^5$)** | **GF($3^7$)** | **GF($7^7$)** |
| **Number of IPs.** | 48 | 3360 | 312 | 117648 |

## 4. Conclusion.

To the best knowledge of the present authors, there is no mention of a paper in which the composite polynomial method is translated into an algorithm and turn into a computer program. The new algorithm is a much simpler to find Monic IPs over Galois Field GF($p^q$). It is able to determine decimal equivalents of the Monic IPs over Galois Field with a large value of prime modulus, also with large extensions of the prime modulii. So this method can reduce the time complexity to find monic Irreducible Polynomials over Galois Field with large value of prime modulii and also with large extensions of the prime modulii. So this would help the crypto community to build S-Boxes or ciphers using irreducible polynomials over Galois Fields with a large value of prime modulii, also with the large extensions of the prime modulii.

**References:**

[1] Church R., “Tables of Irreducible Polynomials for the first four Prime Moduli”, Annals of Mathematics, Vol. 36(1), pp. 198 – 209, January, 1935.

[2] Jacques C’almet And Riidiger Loos, “An Improvement of Rabin’s Probabilistic Algorithm For Generating Irreducible Polynomials Over Gf(P)”, Information Processing Letters, 20 October 1980, Volume 11, No. 2.

[3] Zaman , J K M Sadique Uz, Dey sankhanil, Ghosh, R, “An Algorithm to find the Irreducible Polynomials over Galois Field GF($p^m$)”, International Journal of Computer Applications (0975 – 8887) Volume 109 – No. 15, January 2015.

[4] Adleman L.M. and Lenstra H.W., “Finding irreducible polynomials over finite fields”, Proc. 18th ACM Conf. on The Theory of Computing, Berkeley, CA, pp. 350 – 355., 1986.

[5] Lidl, R, Niederreiter, H, Finite Fields, Encyclopedia of Mathematics and its Applications, Vol. 20, Addison-Wesley Publishing Company, 1983.

PeerJ Preprints | https://doi.org/10.7287/peerj.preprints.3258v1 | CC BY 4.0 Open Access | rec: 17 Sep 2017, publ: 17 Sep 2017