Positional Arithmetic: Subtraction, Multiplication and Division over Extended Galois Field GF(p^q).

Sankhanil Dey[1] and Ranjan Ghosh[2],
sankhanil12009@gmail.com, rghosh47@yahoo.co.in,
Institute of Radio Physics and Electronics,
92 APC Road, Kolkata-700009,
University of Calcutta.

Abstract. The method to Subtract, Multiply and Divide two Field Numbers over the Extended Galois Field GF(p^q) is a well needed solution to the field of Discrete Mathematics as well as in Cryptology. In this paper the addition of two Galois Field Numbers over Extended Galois Field GF(p^q) has been reviewed and Subtraction, Multiplication and Division of two Galois Field Number over Extended Galois Field GF(p^q) has been defined.

Introduction. In Galois field addition [1][2] two digits of two different Galois field number of the same position have been added in decimal and modulated with Galois field Prime Modulus P to obtain the respective digits of the Sum Galois field Number over Galois Field GF(p^q) . In Galois field subtraction digits of the less valued Galois field number from the greater valued Galois field number of the same position have been subtracted in decimal and modulated with Galois field Prime Modulus P to obtain the respective digits of the Difference Galois field Number over Galois Field GF(p^q).

In Multiplication of two Galois Field Numbers over extended Galois field GF(p^q) The product Number must have $(q_1+q_2)+1$ digits in it if 1st number contains q1 positions and 2nd number contains q_2 positions. The position of the terms of the Product Number over extended Galois field GF(p^q) varies from $0 \rightarrow (q_1+q_2)$. The product of the terms of each multiplicand and multiplier Galois field number over extended Galois field GF(p^q) having positions $0 \rightarrow (q_1+q_2)$ have been added and modulated by prime of the respective Galois field to obtain the terms in each position of the Product Number over extended Galois field GF(p^q).

In Division of two Galois Field Numbers over Extended Galois field GF(p^q) N_1 and N_2, the digit in q_1+1^{th} position of Dividend N_1 since $N_1 \geq N_2$ has been divided by the digit in q_2+1^{th} position of Divisor N_2 to obtain the quotient in (q_1--q_2+1) position . The Divisor N_2 is Multiplied over Galois Field GF(p^q) with Quotient and Subtracted over Galois Field GF(p^q) from Dividend to obtain the Remainder. If Remainder $\geq N_2$ then continue the process with the digit in $(q_1+1-i)^{th}$ position of Dividend N_1 where $0 \leq i \leq (q_1--q_2)$ until 0=Remainder< N_2.

Since this arithmetic Deals with Positions of the Galois field numbers over Galois Field GF(p^q) so it is termed as Positional Arithmetic.

Addition and Subtraction operation on two Galois Field Numbers over Extended Galois Field GF(p^q) has been reviewed and described together in section. 2. The Multiplication and Division of two Galois Field Number over Extended Galois Field GF(p^q) have been define in section 3, and 4 respectively. The conclusion and References of the paper has been given in section 5 and 6 respectively.

2. Review and description of arithmetic operations Addition and Subtraction of two Galois field number over Extended Galois Field GF(p^q).

Let N_1 and N_2 or $N_1(p)$ and $N_2(p)$ are two Galois Field numbers or Galois Field Polynomials over Extended Galois Field GF(p^q) respectively. The relation between two Galois field Numbers and Galois field Polynomials with highest degree d € q have been described as follows. Let $\mathbf{N_1}(p)$ and N2(p) are two Galois field polynomials over Extended Galois Field GF(p^q) and coefficients of them have been given as follows,

$\mathbf{N_1}(p) = CO_{N1}{}^{q}, CO_{N1}{}^{q-1}, CO_{N1}{}^{q-2}, CO_{N1}{}^{q-3}, \ldots\ldots\ldots\ldots\ldots\ldots.., CO_{N1}{}^{0} \ldots\ldots\ldots.(1P)$

$\mathbf{N_2}(p) = CO_{N2}{}^{q}, CO_{N2}{}^{q-1}, CO_{N2}{}^{q-2}, CO_{N2}{}^{q-3}, \ldots\ldots\ldots\ldots\ldots\ldots.., CO_{N2}{}^{0} \ldots\ldots\ldots.(2P).$

Then the array of all coefficients from MSB to LSB, constitutes the Galois field Numbers $\mathbf{N_1}$ and $\mathbf{N_2}$ have been given as,

$\mathbf{N_1} = CO_{N1}{}^{q} - CO_{N1}{}^{q-1} - CO_{N1}{}^{q-2} - CO_{N1}{}^{q-3}, \ldots\ldots\ldots\ldots\ldots\ldots.., CO_{N1}{}^{0} \ldots\ldots\ldots.(1N)$

$\mathbf{N_2} = CO_{N2}{}^{q} - CO_{N2}{}^{q-1} - CO_{N2}{}^{q-2} - CO_{N2}{}^{q-3}, \ldots\ldots\ldots\ldots\ldots\ldots.., CO_{N2}{}^{0} \ldots\ldots\ldots.(2N).$

Now if $ADD(N_1(p),N_2(p))$ is the Summation Polynomial over Extended Galois Field GF(p^q) of $N_1(p)$ and $N_2(p)$ and $ADD(N_1,N_2)$ is the sum of N_1 and N_2, then The coefficients of the summation Polynomial and Each digit of the Summed Number from MSB to LSB then,

$$ADD(N_1(p),N_2(p)) = \sum_{q = q \text{ to } 0} (CO_{N1}{}^{q} + CO_{N2}{}^{q}) \bmod p \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots(3P)$$

$ADD(N_1,N_2) = (CO_{N1}^{q} + CO_{N2}^{q}) \bmod p$ where $0 \le q \le q$……...(3N)

Now if $SUB(N_1(p),N_2(p))$ is the Subtracted Polynomial over Extended Galois Field $GF(p^q)$ of $N_1(p)$ and $N_2(p)$ where $N_1(p) \ge N_2(p)$. and $SUB(N_1,N_2)$ is the subtraction of N_1 and N_2 where $N_1 \ge N_2$, then The coefficients of the subtracted Polynomial and Each digit of the Subtracted Number from MSB to LSB then,

$SUB(N_1(p),N_2(p)) = \sum_{q=q\ to\ 0} (CO_{N1}^{q} -- CO_{N2}^{q}) \bmod p$…… ..(4P)

$SUB(N_1,N_2) = (CO_{N1}^{q} -- CO_{N2}^{q}) \bmod p$ where $0 \le q \le q$……..(4N)

3. Multiplication of two Galois field numbers over Extended Galois Field $GF(p^q)$.

Let N_1 and N_2 or $N_1(p)$ and $N_2(p)$ are two Galois Field numbers or Galois Field Polynomials over Extended Galois Field $GF(p^q)$. The relation between two Galois field Number and Galois field Polynomials with highest degree d Є q have been described as follows. Let $\mathbf{N_1}(p)$ and $N_2(p)$ are two Galois field polynomials over Extended Galois Field $GF(p^q)$ and coefficients of them have been given as follows,

$\mathbf{N_1}(p) = CO_{N1}^{q}, CO_{N1}^{q-1}, CO_{N1}^{q-2}, CO_{N1}^{q-3}$,……..., CO_{N1}^{0}……..(5P)

$\mathbf{N_2}(p) = CO_{N2}^{q}, CO_{N2}^{q-1}, CO_{N2}^{q-2}, CO_{N2}^{q-3}$,……..., CO_{N2}^{0}……..(6P).

Then the array of all coefficients constitutes the Galois field Numbers $\mathbf{N_1}$, $\mathbf{N}$, have been given as,

$\mathbf{N_1} = CO_{N1}^{q} - CO_{N1}^{q-1} - CO_{N1}^{q-2} - CO_{N1}^{q-3}$,……..., CO_{N1}^{0}……..(5N)

$\mathbf{N_2} = CO_{N2}^{q} - CO_{N2}^{q-1} - CO_{N2}^{q-2} - CO_{N2}^{q-3}$,……..., CO_{N2}^{0}……..(6N).

Now if $MUL(N_1(p),N_2(p))[d]$ is the Product Polynomial over Extended Galois Field $GF(p^q)$ of $N_1(p)$ and $N_2(p)$ and $MUL(N_1,N_2)[T]$ is the product of N_1 and N_2, then The coefficients of the Product Polynomial and Each digit of the Product Number from MSB to LSB then,

$MUL(N_1(p),N_2(p))\ [2q] = (CO_{N1}^{q} \times CO_{N2}^{q}) \bmod p;$

$MUL(N_1(p),N_2(p))\ [2q-1] = (CO_{N1}^{q-1} \times CO_{N2}^{q} + CO_{N1}^{q} \times CO_{N2}^{q-1}) \bmod p;$

$MUL(N_1(p),N_2(p))\ [2q-2] = (CO_{N1}^{q-2} \times CO_{N2}^{q} + CO_{N1}^{q-1} \times CO_{N2}^{q-1} + CO_{N1}^{q} \times CO_{N2}^{q-2}) \bmod p;$

……

……

$MUL(N_1(p),N_2(p))\ [0] = (CO_{N1}^{0} \times CO_{N2}^{0}) \bmod p;$

Now for two Galois Field Numbers over Extended Galois Field $GF(p^q)$,

$MUL(N_1,N_2)\ [2q] = (CO_{N1}^{q} \times CO_{N2}^{q}) \bmod p;$

$MUL(N_1,N_2)\ [2q-1] = (CO_{N1}^{q-1} \times CO_{N2}^{q} + CO_{N1}^{q} \times CO_{N2}^{q-1}) \bmod p;$

$MUL(N_1,N_2)\ [2q-2] = (CO_{N1}^{q-2} \times CO_{N2}^{q} + CO_{N1}^{q-1} \times CO_{N2}^{q-1} + CO_{N1}^{q} \times CO_{N2}^{q-2}) \bmod p;$

……

……

$MUL(N_1,N_2)\ [0] = (CO_{N1}^{0} \times CO_{N2}^{0}) \bmod p;$

Then the Product of two Galois field Polynomials over Extended Galois Field $GF(p^q)$ where x is denoted as variable and product of two Galois Field Numbers over Extended Galois Field $GF(p^q)$ has been given as,

$MUL(N_1(p),N_2(p)) = MUL(N_1(p),N_2(p))\ [2q]\ x^{2q+1} + MUL(N_1(p),N_2(p))\ [2q-1]\ x^{2q} + ... + MUL(N_1(p),N_2(p))\ x^{0}\ [0].$

$MUL(N_1,N_2) = MUL(N_1,N_2)\ [2q] - MUL(N_1,N_2)\ [2q-1] - MUL(N_1,N_2)\ [2q-2] - \ldots\ldots\ldots\ldots - MUL(N_1,N_2)\ [0].$

4. Division of two Galois field numbers over Extended Galois Field $GF(p^q)$.

If $Qnt(N_1,N_2)$ and $Rem(N_1,N_2)$ of N_1 and N_2 where $N_1 \ge N_2$ are the Quotient and Remainder Galois Field Numbers respectively over Galois field $GF(p^q)$ of N_1 divided by N_2 and Multiplicative Inverse of each digit of N_2 has been denoted as a Galois Field Number over Galois field $GF(p^q)$ M_2 then,

$Qnt(N_1,N_2)[pos\ N_1\text{- }pos\ N_2+1] = (CO_{N1}^{q}/(\ CO_{N2}^{q} * CO_{M2}^{q}))* CO_{M2}^{q}.$
$rem(N_1,N_2)[pos\ N_1\text{- }pos\ N_2+1] = N_1\text{- }Qnt(N_1(p),N_2(p))[pos\ N_1\text{- }pos\ N_2]* N_2.$
If $rem(N_1,N_2)[pos\ N_1\text{- }pos\ N_2+1] \geq N_2$ then,
$N_1 = rem(N_1,N_2)[pos\ N_1\text{- }pos\ N_2+1].$
$Qnt(N_1,N_2)[pos\ N_1\text{- }pos\ N_2] = (CO_{N1}^{q-1}/(\ CO_{N2}^{q-1} * CO_{M2}^{q-1}))* CO_{M2}^{q-1}.$
$rem(N_1,N_2)[pos\ N_1\text{- }pos\ N_2] = N_1\text{- }Qnt(N_1,N_2)[pos\ N_1\text{- }pos\ N_2]* N_2.$
Operation is going on Untill $rem(N_1,N_2)=0$; or
$rem(N_1,N_2)[pos\ N_1\text{- }pos\ N_2] < N_2$

5. Conclusion. In this paper a new Arithmetic Procedure to subtract, Multiply and divide two Galois Field Numbers over Galois Field $GF(p^q)$ have been defined. These procedures have been defined and successfully tested with examples. This work is very useful and utmost related and opens a new way in Discrete Mathematics, Cryptography, Physics and Computer Science.

6. References.

[1]"Galois' Theorem and Polynomial Arithmetic", Chap:4 Finite Fields,
Link: http://www.doc.ic.ac.uk/~mrh/330tutor/ch04s02.html.
[2] Benvenuto, Christoforus Juan, "Galois Field in Cryptography" May 31, 2012,
Link: https://www.math.washington.edu/~morrow/336_12/papers/juan.pdf.
[3] W. H. Bussey (1905) "Galois field tables for $p^n \leq 169$", Bulletin of the American Mathematical Society 12(1): 22–38, doi:10.1090/S0002-9904-1905-01284-2.
[4] W. H. Bussey (1910) "Tables of Galois fields of order < 1000", Bulletin of the American Mathematical Society 16(4): 188–206, doi:10.1090/S0002-9904-1910-01888-7.
[5] Jacobson, Nathan (2009) [1985], Basic algebra I (Second ed.), Dover Publications, ISBN 978-0-486-47189-1.
[6] Mullen, Gary L.; Mummert, Carl (2007), Finite Fields and Applications I, Student Mathematical Library (AMS), ISBN 978-0-8218-4418-2.
[7] Mullen, Gary L.; Panario, Daniel (2013), Handbook of Finite Fields, CRC Press, ISBN 978-1-4398-7378-6.
[8] Lidl, Rudolf; Niederreiter, Harald (1997), Finite Fields (2nd ed.), Cambridge University Press, ISBN 0-521-39231-4