ISSN 2347-1921
Volume 12 Number 07
Journal of Advances in Mathematics

A REDUCED TABLEOF THE ZECH´S LOGARITHM

O. C. Justiz[1], E. M. Capó[2], P. F. Arrozarena[3], G. S. Gómez[4]
Departament of Mathematics. Central University "Marta Abreu" of Las Villas. Cuba
oristela@uclv.edu.cu
Departament of Mathematics. Central University "Marta Abreu" of Las Villas. Cuba
evaristoj@uclv.cu
Habana University. Cuba
pfreyre@matcom.uh.cu
Center ofMathematics Research. Guanajuato. México
guillermo.sosa@cimat.mx

ABSTRACT

In this work we will solve the problem of expression of the sum of two given elements of a finite field, as power of the primitive element of the field. We obtain a reduced table of the Zech's logarithm from our proposal that relate the Zech'slogarithm with the partition of the exponents of the powers of elements over finite field $\boldsymbol{GF(p^n)}$ in p-cyclotomic cosets modulo $(\boldsymbol{p^n-1})$. This reduces, in a significant way, the quantity of information to store and it facilitates its use in several cryptographic algorithms, specifically in asimetric cryptography. It is illustrated the computationof the Zech'slogarithm of any element thatdoesn't appear in the obtained reduced table.

Indexingterms/Keywords

Finite field; Zech's logarithm; cyclotomiccoset.

Academic Discipline And Sub-Disciplines

Discipline: Matthematics, Computer Science.Sub-Disciplines: Cryptology, Theoretical Computer Science.

MATHEMATICS SUBJECTCLASSIFICATION

MSC 2010:12E30, 11T22, 11T71

INTRODUCTION

The study of finite fields has made great progress in recent years because they are applied in areas as diverse as cryptography [1, 2, 3], coding theory [4, 5, 6], among other areas [7, 8]. By working with finite fields, arithmetic operations with its elements are performed, so you need to have efficient algorithms to perform such operations, this being a major problem today.

Considering that multiplication of elements of a finite field is a polynomial multiplication it is convenient express the elements of the field as powers of a primitive element, so that the multiplication of them is reduced to the sum of their exponents. Also is necessary have a procedure to perform efficiently the sum of two elements of the field expressed as a power of the primitive element, since this operation under the above condition is not trivial. To solve this the so-called Zech´s logarithm table [6] is used.

Another related problem with the above is when there are two binary finite fields $GF(2^n)$ and $GF(2^m)$ with primitive elements isα andβrespectively (GF, denote Galois Field). All elements of $GF(2^n)$ and $GF(2^m)$can be expressed as powers of α andβrespectively. The elements of both fields can also be expressed as a binary digit sequence of n and m respectively. If we add $m-n$ bits to the right of the elements α^iwe obtain 2^{m-n}sequences of m digits .An interesting question is ¿How to determine wichpower of the primitive element β, over the field $GF(2^m)$, representthese new sequences?

In this paper a proposal that significantly reduces the Zech's logarithm table is presented.

APPROACH PROBLEMS

Problem 1

Let the finite field $GF(2^n)$ which is an algebraic extension of degree n of the prime field $GF\ (p)$.We want to find the pairs (i,j) satisfying,

$$1+\alpha^i=\alpha^j \quad (1)$$

Considering that in any finite field of characteristic p [8].

$$(1+\ \alpha^i)^{\mathrm{p}}=(\alpha^j)^p \Rightarrow 1+\alpha^{ip}=\alpha^{jp} \quad (2)$$

$$(1+\ \alpha^i)^{\mathrm{p}^k}=(\alpha^j)^{\mathrm{p}^k} \Rightarrow 1+\alpha^{ip^k}=\alpha^{jp^k} \quad (3)$$

is satisfied. Then if the pair (i,j) satisfies the relation (1) then the pair $(i \times p^k,\ j \times p^k)$also satisfies. The $i \times p^k$y $j \times p^k$elements are reduced modulo $p^n - 1$.How to find these pairs?

Problem 2

Suppose we have the finite field $GF(q)$= $GF(p^n)$where p is a prime number and n is a positive integer. Let α a primitive element of the field $GF(p^n)$.If there are two elements of a finite field expressed as powers of the primitive element, how to express their sum as a power of the primitive element ?.

In other words. If i,j,k are non-negative integers such numbers that $i \neq j \neq k$y $i \neq j \neq 0$,if$\alpha^i + \alpha^j = \alpha^k$. How to find k?.

If in the expression $\alpha^i + \alpha^j$we extract the common factor under the powers we can reduce the problem to the previous case.

Suppose that $i < j$, we have, with $v = (j-i) \bmod (p^n - 1)$,

$$\alpha^i + \alpha^j = \alpha^i\ (1 + \alpha^v)$$

then,

$$1 + \alpha^v = \alpha^r \rightarrow \alpha^i \cdot \alpha^r = \alpha^{(i+r) \bmod (p^n-1)}$$

To answer this questions these problems for $GF(p^n)$and$n = \overline{2,8}$fields were resolved. The results enabled us to detect regularities that allow us to build a reduced table ofZech'slogarithm, considering the p–cyclotomiccosetsmodulo $p^n - 1$.

Let α a generator element of the multiplicative group of the field $GF(p^n)$, the product of two elements of the finite field are represented by$\alpha^i \cdot \alpha^j = \alpha^{(i+j) \bmod (p^n-1)}$ and the addition of the elements of the finite field expressed as powers ofprimitive element is facilitated if the calledZech'slogarithm table is built [6], where for each integer $i, 0 \leq i \leq p^{n-2}$, the integer$j = z(i)$such that

$$1 + \alpha^i = \alpha^j = \alpha^{z(i)} \qquad (4)$$

is determined. Then,

$$\alpha^i + \alpha^j = \alpha^i \cdot (1 + \alpha^v) = \alpha^i \cdot \alpha^{z(j-i)} = \alpha^{i+z(v)},$$

where$z(v)$is taken from the Zech's logarithm table.

Given (4) and the analysis in the problem statement,the expressions (2) and (3) can be rewritten as follows

$$(1 + \alpha^i)^p = \alpha^{z(i)\,p} \Rightarrow 1 + \alpha^{ip} = \alpha^{p \times z(i)}$$

$$(1 + \alpha^i)^{p^k} = \alpha^{z(i)\,p^k} \Rightarrow 1 + \alpha^{ip^k} = \alpha^{p^k \times z(i)}$$

RELATIONSHIP BETWEEN THEZECH'S LOGARITHMAND THE CYCLOTOMIC COSETS

We began recall that the q-cyclotomiccosets[9] [10] of S modulo $n$is defined by the set $C_s = \{s, sq, sq^2, \cdots, sq^{r-1}\}$, where r is the smallest positive integer such that $sq^r \equiv s \pmod n$. In particular, the2–cyclotomiccoset[9] [10]modulo$n$ is the set$C_s = \{s, s2, s2^2, \cdots, s2^{r-1}\}$, where r is the smallest positive integer such that $s2^r \equiv s \pmod n$.

We noted earlier thatif the pair (i,j) satisfies the relation(1) then the pair $(i \times p^k, j \times p^k)$also satisfies it .The expression$i \times p^k\ (mod\ (p^n - 1))$where $i \in [0,r]$represents all the elements that arein the same p-cyclotomiccosetmodulo $p^n - 1$.Thereforeknowing the Zech'slogarithm of an integer i we can find the Zech's logarithm ofallintegers of the form $i \times p^k\ (mod\ (p^n - 1))$.

We illustrate the above taking a particular finite field.

Let the finite field $GF(2^8)$we take primitive polynomial$x^8 + x^4 + x^3 + x^2 + 1$as the defining polynomial. Letαbe a root of this polynomialand hence a primitive field element.

The2–cyclotomiccosets [9] modulo 255 are as follows

C_0 = {0}

C_1={1,2,4,8,16,32,64,128}

C_3={3,6,12,24,48,96,192,129}

C_5={5,10,20,40,80,160,65,130}

C_7={7,14,28,56,112,224,193,131}

C_9={9,18,36,72,144,33,66,132}

C_{11}={11,22,44,88,176,97,194,133}

C_{13}={13,26,52,104,208,161,67,134}

C_{15}={15,30,60,120,240,225,195,135}

C_{17}={17,34,68,136}

C_{19}={19,38,76,152,49,98,196,137}

C_{21}={21,42,84,168,81,162,69,138}

C_{23}={23,46,92,184,113,226,197,139}

C_{25}={25,50,100,200,145,35,70,140}

C_{27}={27,54,108,216,177,99,198,141}

C_{29}={29,58,116,232,209,163,71,142}

C_{31}={31,62,124,248,241,227,199,143}

C_{37}={37,74,148,41,82,164,73,146}

C_{39}={39,78,156,57,114,228,201,147}

C_{43}={43,86,172,89,178,101,202,149}

C_{45}={45,90,180,105,210,165,75,150}

C_{47}={47,94,188,121,242,229,203,151}

C_{51}={51,102,153,204}

C_{53}={53,106,212,169,83,166,77,154}

C_{55}={55,110,220,185,115,230,205,155}

C_{59}={59,118,236,217,179,103,206,157}

C_{61}={61,122,244,233,211,167,79,158}

C_{63}={63,126,252,249,243,231,207,159}

C_{85}={85,170}

C_{87}={87,174,93,186,117,234,213,171}

C_{91}={91,182,109,218,181,107,214,173}

C_{95}={95,190,125,250,245,235,215,175}

C_{111}={111,222,189,123,246,237,219,183}

C_{119}= {119,238,221,187}

C_{127}={127,254,253,251,247,239,223,191}

The cosetsC_{17},C_{51},C_{85},C_{119} are the regular cyclotomiccosets [10] .In this case we have 35 cyclotomiccosetsdenoted by $C_i$where i is the coset leaders0 ≤ i ≤ 127. So,i is a positive integer that takes values in the range from 0 to $\frac{p^n-1}{2}$.

Thetable of Zech's logarithm for the field $GF(2^8)$with defining polynomial $x^8+x^4+x^3+x^2+1$,grouping the values of$j$ according to the cyclotomic coset that they belong, appears in the Annex.

Here are some examples of computation the sum of two elements of a finite field using Zech's logarithm table.

Example1:

a. $\alpha^7+\alpha^{47}=\alpha^7\cdot(1+\alpha^{40})=\alpha^7\cdot(1+\alpha^{5\times 2^3})=\alpha^7\cdot(1+\alpha^5)^{2^3}=\alpha^7\cdot\alpha^{z(5)\times 8\ (mod\ 255)}$

$=\alpha^7\cdot\alpha^{138\times 8\ (mod\ 255)}=\alpha^{7+84}=\alpha^{91}$

b. $\alpha^{37}+\alpha^{103}=\alpha^{37}\cdot(1+\alpha^{66})=\alpha^{37}\cdot(1+\alpha^{33\times 2})=\alpha^{37}\cdot(1+\alpha^{33})^2=\alpha^{37}\cdot\alpha^{z(33)\times 2\ (mod\ 255)}$

$=\alpha^{37}\cdot\alpha^{15\times 2\ (mod\ 255)}=\alpha^{67}$

c. $\alpha^{219}+\alpha^{135}=\alpha^{135}\cdot(1+\alpha^{84})=\alpha^{135}\cdot(1+\alpha^{21\times 2^2})=\alpha^{135}\cdot(1+\alpha^{21})^{2^2}=\alpha^{135}\cdot\alpha^{z(21)\times 4\ (mod\ 255)}$

$=\alpha^{135}\cdot\alpha^{40}=\alpha^{175}$

Now we buildthe table of theZech's logarithm given the partition of the set of non-negative integers $\{0,1,2,3,\cdots,254\}$ in 2–cyclotomiccosetsmodulo255. This allows us not store the entire table but only the values of the Zech's logarithm for the coset leaders.

The Zech´s logarithm for the finite field $GF(2^8)$ with defining primitive polynomial $x^8+x^4+x^3+x^2+1$,considering onlythe coset leaders, is showed in the following table.

Table 1: 2–cyclotomiccosets modulo 255

j	z(j)	j	z(j)	j	z(j)	j	z(j)
0	∞	15	33	39	106	63	55
		17	68	43	121	85	170
1	25	19	92	45	31	87	167
3	223	21	10	47	101	91	209
5	138	23	196	51	238	95	176
7	112	25	1	53	147	111	246
9	120	27	104	55	63	119	153
11	245	31	45	59	82	127	12
13	99	37	179	61	186		

Using the table of coset leaders to calculate Zech's logarithm of a value of d that is not on the table. The following cases may arise:

1. The number d is the product of a power of the characteristic field and an odd number which is a coset leader.

2. The number d is an odd number that is not a coset leader.
3. The number d is the product of a power of the characteristic field and an odd number which that is not a coset leader.

Case 1:

If $\boldsymbol{d = i \times p^k}$ then $\boldsymbol{z(d) = z(i) \times p^k (\mathrm{mod}(p^n - 1))}$

Case 2:

We add $\boldsymbol{(p^n - 1)}$ to $\boldsymbol{d}$ and expressed as the product of the largest possible power of thecharacteristicfieldand an odd number,

$$\boldsymbol{d + (p^n - 1) = d_1 \rightarrow d_1 = d_2 \times p^{k_1} \rightarrow d_2 + (p^n - 1) = d_3 \rightarrow d_3 = d_4 \times p^{k_2} \rightarrow \cdots}$$

Suppose that for $\boldsymbol{r}$ is obtained :

$$\boldsymbol{d_{r-1} = d_r \times p^{\frac{k_r}{2}}}$$

where $\boldsymbol{d_r}$ is a coset leader.Stop the process and

$$\boldsymbol{d = d_r \times p^{k_1} \times p^{k_2} \times \cdots \times p^{\frac{k_r}{2}} = d_r \times p^k} \text{ being } \boldsymbol{k = k_1 + k_2 + \cdots + \frac{k_r}{2}}, \text{ with } \boldsymbol{k_1, k_2, \cdots, \frac{k_r}{2}} \in [0, \boldsymbol{n - 1}].$$

$\boldsymbol{z(d) = z(d_r) \times p^k}$ $(\mathrm{mod}(\boldsymbol{p^n - 1})) = \boldsymbol{z(i) \times p^k}$ $(\mathrm{mod}(\boldsymbol{p^n - 1}))$ for same cosetleader $\boldsymbol{i}$.

Case 3:

If $\boldsymbol{d = d_1 \times p^{k_1}}$, we proceed to $\boldsymbol{d_1}$ similarly to Case 2.

Example 2:

Compute in $GF(2^8)$,

a) $z(168) = z(21) \times 2^3 \pmod{255} = 10 \times 8 = 80$

b) $z(197)$

197 is an odd number that is not a coset leader

$197 + 255 = 452 \rightarrow 452 = 113 \times 2^2 \rightarrow 113 + 255 = 368 \rightarrow 368 = 23 \times 2^4$

As23 is a cosetleader then

$197 \equiv 23 \times 2^2 \times 2^4 \pmod{255} = 23 \times 2^6 \pmod{255} \equiv 226$

$z(197) = z(23 \times 2^6 \pmod{255}) = z(23) \times 2^6 \pmod{255} = 196 \times 64 \pmod{255} \equiv 49$

c) $z(228)$

$228 = 57 \times 2^2 \rightarrow 57 + 255 = 312 \rightarrow 312 = 39 \times 2^3$

39 is a cosetleader

$228 \equiv 39 \times 2^2 \times 2^3 \pmod{255} = 39 \times 2^5 \pmod{255}$

$z(228) \equiv z(39) \times 2^5 \pmod{255} = 106 \times 32 \pmod{255} = 77$

CONCLUSIONS

In this paper a modification to the table of Zech´s logarithm for the field $GF(2^8)$, applicable to any given field, consisting of a considerable reduction of the number of elements to be stored is proposed. For this the called p-cyclotomic cosets were used. This result is essential to perform the addition operation between two elements of a finite field represented as powers of a primitive element of this field. It also has various applications in cryptography, especially in the implementation of cryptographic algorithms.

REFERENCES

1. Didier F., M. and Laigle-ChapuyY.2007. Finding low-weight polynomial multiples using discrete logarithm.
2. Johansson T.2014.Low weight polynomials in crypto.

3. Kiihn G. J. and W. Penzhorn T. 1994. Using Zech's Logarithm to Find Low-Weight Parity Checks for Linear Recurring Sequences. Communications and cryptography.
4. Elsenhans A.-S., KohnertA. and Wassermann A. 2010. Construction of Codes for Network Coding. In Proceedings of the 19th International Symposium on Mathematical Theory of Networks and Systems – MTNS 2010.
5. LiJ. 2004. Combinatorially Designed LDPC Codes Using Zech Logarithms and Congruential Sequences.Coding, Cryptographyand Combinatorics.
6. Huber K.1990. Some Comments on Zech's Logarithms. IEEE Transactions on Information Theory.
7. Meyer-Baese U. 2004. Digital Signal Processing with Field Programmable Gate Arrays. SecondEdition.
8. MullenG. L.and Panario D.2013. Handbook of Finite Fields, CRC Pres.Taylor& Francis Group.
9. Golomb S. W. 1981. Shift Register Sequences, Aegean Park Press. Laguna Hills, CA, USA.
10. Rani M. J. 2013 Cyclic Codes of length N over GF(q)q- ciclotomiccosets modulo N and application of Burnside´s lemma. InternationalJournal of Scientific and Research Publications.

ANEX

Table of the Zech´slogarithm forthe finite field$GF(2^8)$with definingprimitive polynomial$x^8+x^4+x^3+x^2+1$

$1+\alpha^i=\alpha^{z(i)}$

i	$z(i)$	i	$z(i)$	i	$z(i)$	i	$z(i)$
1	25	3	223	5	138	7	112
2	50	6	191	10	21	14	224
4	100	12	127	20	42	28	193
8	200	24	254	40	84	56	131
16	145	48	253	80	168	112	7
32	35	96	251	160	81	224	14
64	70	192	247	65	162	193	28
128	140	129	239	130	69	131	56
i	$z(i)$	i	$z(i)$	i	$z(i)$	i	$z(i)$
9	120	11	245	13	99	15	33
18	240	22	235	26	198	30	66
36	225	44	215	52	141	60	132
72	195	88	175	104	27	120	68
144	135	176	95	208	54	240	136
33	15	97	190	161	108	225	17
66	30	194	125	67	216	195	34
132	60	133	250	134	177	135	68
17	68	51	238	85	170	119	153
34	136	102	221	170	85	238	51
68	17	204	187	∞	0	221	102
136	34	153	119	0	∞	187	204
19	92	21	10	23	196	25	1
38	184	42	20	46	137	50	2

76	113	84	40	92	19	100	4
152	138	168	80	184	38	200	8
49	197	81	160	113	76	145	16
98	139	162	65	226	152	35	32
196	23	69	130	197	49	70	64
137	46	138	5	139	98	140	128
27	104	29	181	31	45	37	179
54	208	58	107	62	90	74	103
108	161	116	214	124	180	148	206
216	67	232	173	248	105	41	157
177	134	209	91	241	210	82	59
99	13	163	182	227	165	164	179
198	26	71	109	199	75	73	103
141	52	142	218	143	150	146	206
39	106	43	121	45	31	47	101
78	212	86	242	90	62	94	202
156	169	172	229	180	124	188	149
57	83	89	203	105	248	121	43
114	166	178	151	210	241	242	86
228	77	101	47	165	227	229	172
201	154	202	94	75	199	203	89
147	53	149	188	150	143	151	178
53	147	55	63	59	82	61	186
106	39	110	126	118	164	122	117
212	78	220	252	236	73	244	234
169	156	185	249	217	146	233	213
83	57	115	243	179	37	211	171
166	114	230	231	103	74	167	87
77	228	205	207	206	148	79	174
154	201	155	159	157	41	158	93

i	$z(i)$	i	$z(i)$	i	$z(i)$	i	$z(i)$
87	167	91	209	95	176	11	246
174	79	182	163	190	97	222	237
93	158	109	71	125	194	189	219
186	61	218	142	250	133	123	183
117	122	181	29	245	11	246	111
234	244	107	58	235	22	237	222
213	233	214	116	215	44	219	189
171	211	173	232	175	88	183	123
127	12	253	48	247	192	223	3
254	24	251	96	239	129	191	6