Abstract Algebra

Introduction to Finite Field

We can define $GF(5)$ on the set Z_5 (5 is a prime) with addition and multiplication operators as shown

GF(5)

{0, 1, 2, 3, 4} + ×

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

Addition

×	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Multiplication

Additive inverse

a	0	1	2	3	4
−a	0	4	3	2	1

a	0	1	2	3	4
a^{-1}	—	1	3	2	4

Multiplicative inverse

For the sets of polynomials in $GF(2^n)$, a group of polynomials of degree n is defined as the modulus. Such polynomials are referred to as irreducible polynomials.

Degree	*Irreducible Polynomials*
1	$(x + 1)$, (x)
2	$(x^2 + x + 1)$
3	$(x^3 + x^2 + 1)$, $(x^3 + x + 1)$
4	$(x^4 + x^3 + x^2 + x + 1)$, $(x^4 + x^3 + 1)$, $(x^4 + x + 1)$
5	$(x^5 + x^2 + 1)$, $(x^5 + x^3 + x^2 + x + 1)$, $(x^5 + x^4 + x^3 + x + 1)$, $(x^5 + x^4 + x^3 + x^2 + 1)$, $(x^5 + x^4 + x^2 + x + 1)$

Example

Let us define a $GF(2^2)$ field in which the set has four 2-bit words: $\{00, 01, 10, 11\}$. We can redefine addition and multiplication for this field in such a way that all properties of these operations are satisfied, as shown in.

An example of GF(2^2) field

Addition

$\oplus$	00	01	10	11
00	00	01	10	11
01	01	00	11	10
10	10	11	00	01
11	11	10	01	00

Identity: 00

Multiplication

$\otimes$	00	01	10	11
00	00	00	00	00
01	00	01	10	11
10	00	10	11	01
11	00	11	01	10

Identity: 01

The $GF(2^3)$ field has 8 elements. We use the irreducible polynomial $(x^3 + x^2 + 1)$ and show the addition and multiplication tables for this field. We show both 3-bit words and the polynomials. Note that there are two irreducible polynomials for degree 3. The other one, $(x^3 + x + 1)$, yields a totally different table for multiplication.

Let $K = GF(2^4)$, $F = GF(2)$, with defining primitive polynomial $f(x)$ given by

$$f(x) = x^3 + x + 1$$

Then, if α is a root of $f(x)$, we have $f(\alpha)=0$, which implies that

$$f(\alpha) = \alpha^3 + \alpha + 1 = 0$$

This equation over $GF(2)$, means that α satisfies the following equation

$$\alpha^3 = \alpha + 1.$$

Using the above equation, one can now express each one of the 7 nonzero elements of K over F as is shown in the next table.

$GF(2^3)$ Field element generate from $f(x) = x^3 + x + 1$

0	0	000
$\alpha^0 = 1$		001
$\alpha^1 = \alpha^1$		010
$\alpha^2 = \alpha^2$		100
$\alpha^3 = \alpha + 1$		101
$\alpha^4 = \alpha^2 + \alpha$		110
$\alpha^5 = \alpha^2 + \alpha + 1$		111
$\alpha^6 = \alpha^2 + 1$		101

Table 4.6 Polynomial Arithmetic Modulo $(x^3 + x + 1)$

		000	001	010	011	100	101	110	111
	+	0	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
000	0	0	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
001	1	1	0	$x+1$	x	x^2+1	x^2	x^2+x+1	x^2+x
010	x	x	$x+1$	0	1	x^2+x	x^2+x+1	x^2	x^2+1
011	$x+1$	$x+1$	x	1	0	x^2+x+1	x^2+x	x^2+1	x^2
100	x^2	x^2	x^2+1	x^2+x	x^2+x+1	0	1	x	$x+1$
101	x^2+1	x^2+1	x^2	x^2+x+1	x^2+x	1	0	$x+1$	x
110	x^2+x	x^2+x	x^2+x+1	x^2	x^2+1	x	$x+1$	0	1
111	x^2+x+1	x^2+x+1	x^2+x	x^2+1	x^2	$x+1$	x	1	0

(a) Addition

		000	001	010	011	100	101	110	111
	×	0	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
000	0	0	0	0	0	0	0	0	0
001	1	0	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
010	x	0	x	x^2	x^2+x	$x+1$	1	x^2+x+1	x^2+1
011	$x+1$	0	$x+1$	x^2+x	x^2+1	x^2+x+1	x^2	1	x
100	x^2	0	x^2	$x+1$	x^2+x+1	x^2+x	x	x^2+1	1
101	x^2+1	0	x^2+1	1	x^2	x	x^2+x+1	$x+1$	x^2+x
110	x^2+x	0	x^2+x	x^2+x+1	1	x^2+1	$x+1$	x	x^2
111	x^2+x+1	0	x^2+x+1	x^2+1	x	1	x^2+x	x^2	$x+1$

(b) Multiplication

GF(2^4) Field element generate from $f(x) = x^4 + x + 1$

i	α^i	Coordinates
0	1	(0 0 0 1)
1	α	(0 0 1 0)
2	α^2	(0 1 0 0)
3	α^3	(1 0 0 0)
4	$\alpha^4 = \alpha + 1$	(0 0 1 1)
5	$\alpha^5 = \alpha^2 + \alpha$	(0 1 1 0)
6	$\alpha^6 = \alpha^3 + \alpha^2$	(1 1 0 0)
7	$\alpha^7 = \alpha^3 + \alpha + 1$	(1 0 1 1)
8	$\alpha^8 = \alpha^2 + 1$	(0 1 0 1)
9	$\alpha^9 = \alpha^3 + \alpha$	(1 0 1 0)
10	$\alpha^{10} = \alpha^2 + \alpha + 1$	(0 1 1 1)
11	$\alpha^{11} = \alpha^3 + \alpha^2 + \alpha$	(1 1 1 0)
12	$\alpha^{12} = \alpha^3 + \alpha^2 + \alpha + 1$	(1 1 1 1)
13	$\alpha^{13} = \alpha^3 + \alpha^2 + 1$	(1 1 0 1)
14	$\alpha^{14} = \alpha^3 + 1$	(1 0 0 1)

Representation of an 8-bit word by a polynomial(under mod2)

n-bit word	1	0	0	1	1	0	0	1

Polynomial	$1x^7 + 0x^6 + 0x^5 + 1x^4 + 1x^3 + 0x^2 + 0x^1 + 1x^0$
First simplification	$1x^7 + 1x^4 + 1x^3 + 1x^0$
Second simplification	$x^7 + x^4 + x^3 + 1$

Polynomial addition

Let us do $(x^5 + x^2 + x) + (x^3 + x^2 + 1)$ in $GF(2^8)$. We use the symbol Å to show that we mean polynomial addition.

$$
\begin{array}{ll}
0x^7 + 0x^6 + 1x^5 + 0x^4 + 0x^3 + 1x^2 + 1x^1 + 0x^0 & \oplus \\
0x^7 + 0x^6 + 0x^5 + 0x^4 + 1x^3 + 1x^2 + 0x^1 + 1x^0 & \\
\text{---} & \\
0x^7 + 0x^6 + 1x^5 + 0x^4 + 1x^3 + 0x^2 + 1x^1 + 1x^0 & \rightarrow \quad x^5 + x^3 + x + 1
\end{array}
$$

Polynomial Multiplication

Find the result of $(x^5 + x^2 + x) \otimes (x^7 + x^4 + x^3 + x^2 + x)$ in $GF(2^8)$ with irreducible polynomial $(x^8 + x^4 + x^3 + x + 1)$.

$$P_1 \otimes P_2 = x^5(x^7 + x^4 + x^3 + x^2 + x) + x^2(x^7 + x^4 + x^3 + x^2 + x) + x(x^7 + x^4 + x^3 + x^2 + x)$$

$$P_1 \otimes P_2 = x^{12} + x^9 + x^8 + x^7 + x^6 + x^9 + x^6 + x^5 + x^4 + x^3 + x^8 + x^5 + x^4 + x^3 + x^2$$

$$P_1 \otimes P_2 = (x^{12} + x^7 + x^2) \bmod (x^8 + x^4 + x^3 + x + 1) = x^5 + x^3 + x^2 + x + 1$$

Polynomial Divide

$$
\begin{array}{r|l}
 & x^4 + 1 \\
\hline
x^8 + x^4 + x^3 + x + 1 & x^{12} + x^7 + x^2 \\
 & x^{12} + x^8 + x^7 + x^5 + x^4 \\
\cline{2-2}
 & x^8 + x^5 + x^4 + x^2 \\
 & x^8 + x^4 + x^3 + x + 1 \\
\cline{2-2}
\text{Remainder} & \boxed{x^5 + x^3 + x^2 + x + 1}
\end{array}
$$

Multiplication Using Computer

multiplying P1 = $(x^5 + x^2 + x)$ by

P2 = $(x^7 + x^4 + x^3 + x^2 + x)$

in GF(2^8) with irreducible polynomial $(x^8 + x^4 + x^3 + x + 1)$ using the algorithm described above. Note $x^8 = x^4 + x^3 + x + 1$

Powers	*Operation*	*New Result*	*Reduction*
$x^0 \otimes P_2$		$x^7 + x^4 + x^3 + x^2 + x$	No
$x^1 \otimes P_2$	$\boldsymbol{x} \otimes (x^7 + x^4 + x^3 + x^2 + x)$	$x^5 + x^2 + x + 1$	**Yes**
$x^2 \otimes P_2$	$\boldsymbol{x} \otimes (x^5 + x^2 + x + 1)$	$x^6 + x^3 + x^2 + x$	No
$x^3 \otimes P_2$	$\boldsymbol{x} \otimes (x^6 + x^3 + x^2 + x)$	$x^7 + x^4 + x^3 + x^2$	No
$x^4 \otimes P_2$	$\boldsymbol{x} \otimes (x^7 + x^4 + x^3 + x^2)$	$x^5 + x + 1$	**Yes**
$x^5 \otimes P_2$	$\boldsymbol{x} \otimes (x^5 + x + 1)$	$x^6 + x^2 + x$	No
$\mathbf{P_1} \times \mathbf{P_2} = (x^6 + x^2 + x) + (x^6 + x^3 + x^2 + x) + (x^5 + x^2 + x + 1) = \boldsymbol{x^5 + x^3 + x^2 + x + 1}$			

Order	primitive polynomial
3	$1 + x + x^3$
4	$1 + x + x^4$
5	$1 + x + x^5$
6	$1 + x^2 + x^6$
7	$1 + x^3 + x^7$
8	$1 + x^2 + x^3 + x^4 + x^8$
9	$1 + x^4 + x^9$
10	$1 + x^3 + x^{10}$
16	$1 + x + x^3 + x^{12} + x^{16}$

Lab 1

- **MATLAB**

ส่วน1 พหุนาม

ตัวอย่าง ถ้า 1+x^3+x^4

เขียน MATLAB แทนได้

```
>> p1=[1 0 0 1 1 ]
```

ถ้า 1+x+x^3 ?

- พหุนามลดทอนไม่ได้จะเป็นพหุนามปฐมฐาน (primitive polynomial) ลำดับ m ถ้า p(x) นำไปหารด้วยพหุนาม x^n+1 (n=2^m-1) แล้วลงตัว เพียงพหุนามเดียว
- **1**.เขียน MATLAB ทดสอบ

```
>>p1=[1 1 0 1]% 1+x+x^3;
>>p2=[1 0 0 0 0 0 1]%1+x^7;
>>p3=[1 0 0 0 0 1]%1+x^6;
>>[q,r]=gfdeconv(p3,p1);
```

-

- 2. เขียน MATLAB หา primitive polynomial ลำดับ 3 ได้(default)

```
>>m=3

>>poly=gfprimdf(m)
```

จากพหุนามแบบปฐมฐานหน้า 15 ทดสอบตาราง

- 3. การทดสอบ primitive polynomial ลำดับใด ๆ

```
>>poly=[1 1 0 1]
>>gfprimck(poly)
```

-

- 4. แสดงการสร้าง GF(2^3) จากพหุนามปฐมฐาน

```
>>Index=[0;1;2;3;4;5;6]

>>p=2

>>poly=[1 1  0 1]

>>GF=gftuple(index,poly,p)
```

-ทดลองสร้าง GF(2^4)จากพหุนามปฐมฐาน

-สร้างสมาชิกทั้งหมดของ GF(2^4) ด้วยพหุนาม 1+x+x^4 หน้า 9

PYTHON

5.คูณภายใต้primitive polynomial $(x^8 + x^4 + x^3 + x + 1)$ ทดลองคูณ P1xP2 หน้า 12-14

P1 = $(x^5 + x^2 + x)$ = 0x26

P2 = $(x^7 + x^4 + x^3 + x^2 + x)$=0x9e

P1xP2=0x2f

Note Python Bitwise Operator

Binary AND(&) OR(|) XOR(^)

Left-Shift(<<) Right-Shift(>>)

ทดลอง

```
>>>a=0xaa
>>>b=0x55
>>> a&b
>>> a|b
>>> hex(a^0x01)
>>> hex(b<<1)
>>> hex(0x02>>1)
```

ส่วน2 ทฤษฎีจำนวน PYTHON

- 1.โปรแกรมหา gcd จากหนังสือ Crypto for Inf security:
- CIS หน้า 2-3
- **def** gcd(a,b):
-     while a!=0:
-         a,b=b%a,a
-     return b
- จากหนังสือ CIS ในแบบฝึกหัดข้อ 2.หน้า 2-39 เขียนโปรแกรมหา gcd ในแบบ recursive

- 3. จากหนังสือ CIS หน้า 5-8 แสดงโปรแกรมยกกำลัง
- from math import floor
- **def** powermod(a, m, n):
-     x=1
-     while m >=1:
-         if m%2 == 1:
-             x=(x*a)%n
-         a=(a*a)%n
-         m=floor(m/2)
-     return x%n

สำหรับแบบฝึกหัดข้อ 3 หน้า 2-40 หมายเหตุโดยภาษา Python สามารถเขียน a**m%n