Binary Operations

Let G be a set of elements. A *binary operation* ¿ on G is a rule that assigns to each pair of elements *a* and *b* in G a uniquely defined third element *c* = *a* ¿ *b* also in G. When such an operation exists G is said to be *closed* under ¿.

A binary operation ¿ on G is said to be *associative* if for any *a*, *b* and *c* in G:

$$a*(b*c)=(a*b)*c$$

A binary operation ¿ on G is said to be *commutative* if for any *a* and *b* in G:

$$a*b=b*a$$

Groups

A set G on which a binary operation ¿ is defined is called a *group* if the following holds:

i. The binary operation is associative.

ii. *G* contains an element *e* such that for any element *a* in G:

$$a*e=e*a=a$$

The element *e* is called an *identity* of G.

iii. For any element *a* in *G* there exists another element *a'* in *G* such that:

$$a*a'=a'*a=e$$

The element *a'* is called an *inverse* of *a*.

A group G is said to be commutative if its binary operation is commutative.

The number of elements in a group is called the *order* of the group. A group of finite order is called a *finite group*.

A nonempty subset *H* of G is said to be a *subgroup* of G if *H* is closed under the binary operation of G and satisfies all the conditions of a group.

Fields

Let *F* be a set of elements on which two binary operations called addition +¿ and multiplication $\cdot$ are defined. The set *F* and these two binary operations are a *field* if the following holds:

i. *F* is a commutative group under addition. The identity element with respect to addition is called the *zero element* or the *additive identity* of *F* and is denoted by 0.

ii. The set of nonzero elements in *F* is a commutative group under multiplication. The identity element with respect to multiplication is called the *unit element* or the *multiplicative identity* of *F* and is denoted by 1.

iii. Multiplication is *distributive* over addition. For any elements *a*, *b* and *c* in *F*:

$$a\cdot(b+c)=a\cdot b+a\cdot c$$

A field consists of at least two elements, the additive and multiplicative identities.

The number of elements in a field is called the *order* of the field. A field with a finite number of elements is called a *finite field* or a *Galois field* in honor of their discover, Évariste Galois.

The set $\{0,1,2,\ldots,p-1\}$ where *p* is a prime number is a finite field of order *p* under modulo-*p* addition and multiplication. It is denoted by GF(*p*) and is called a *prime field*. For *p* = 2, GF(2) is called a *binary field*.

For any positive integer *m* it is possible to extend the prime field GF(*p*) to a field of p^m elements which is called an *extension field* of GF(*p*) that is denoted by GF(p^m). The order of any finite field is a power of a prime.

For the finite field GF(*q*) there must exist a smallest positive integer such that $\sum_{i=1}^{\lambda} 1=0$. This integer λ is called the *characteristic* of the field GF(*q*) and is itself a prime number.

The sums $\sum_{i}^{j} 1$ for j = 1, 2, ..., λ are distinct elements in GF(*q*) and they form a *subfield* GF(λ¿ of GF(*q*). If $q \neq \lambda$ then *q* is a power of λ.

For GF(*q*) there must exist a smallest positive integer *n* for each nonzero element *a* of GF(*q*) such that $a^n = 1$. This integer *n* is called the *order* of the element *a*. The powers of *a* are all distinct and they form a *cyclic* group under multiplication of GF(*q*).

If *a* is a nonzero element of GF(*q*) then $a^{q-1} = 1$. If *n* is the order of *a* then *n* divides *q* – 1.

In a finite field GF(*q*) a nonzero element *a* is said to be *primitive* if the order of *a* is *q* – 1. The powers of a primitive element generate all the nonzero elements of GF(*q*).

Binary Field Arithmetic

Codes with symbols from the binary field GF(2) or its extension GF(2^m) are the most widely used in digital data transmission and storage.

In binary arithmetic addition and multiplication are modulo-2:

+	0	1
0	0	1
1	1	0

•	0	1
0	0	0
1	0	1

Note that modulo-2 addition is equivalent to logical exclusive OR and modulo-2 multiplication is equivalent to logical AND.

Under modulo-2 addition 1 + 1 = 0 and so 1 = –1. Modulo-2 subtraction is then the same as modulo-2 addition.

A polynomial $f(X)$ with one variable X and coefficients from GF(2) is said to be a polynomial over GF(2) and is of the form:

$$f(X) = f_0 + f_1 X + f_2 X^2 + \ldots + f_n X^n$$

The various f_i are either 0 or 1. The *degree* of the polynomial is the largest power of X with a nonzero coefficient.

Polynomials can be added, subtracted, multiplied and divided the usual way. Calculations of the various coefficients are done using modulo-2 addition and multiplication. Polynomials over GF(2) are commutative, associative and distributive.

When a polynomial $f(X)$ is divided by another polynomial $g(X)$ of nonzero degree two unique polynomials $q(X)$, the quotient, and $r(X)$, the remainder, are generated:

$$f(X)=q(X)g(X)+r(X)$$

The degree of $r(X)$ is less than that of $g(X)$. This is known as Euclid's division algorithm. If the remainder $r(X)$ is identical to zero then $f(X)$ is divisible by $g(X)$ and $g(X)$ is a factor of $f(X)$.

For polynomials over GF(2) if $f(a)$ = 0 then a is a *root* of $f(X)$ and from Euclid's division algorithm $f(X)$ is divisible by $(X+a)$.

A polynomial $p(X)$ over GF(2) of degree *m* is said to be *irreducible* over GF(2) if no polynomial over GF(2) of degree less than *m* but greater than zero divides $p(X)$, that is the polynomial $p(X)$ cannot be factored. For any *m* ≥ 1 there exists an irreducible polynomial over GF(2) of degree *m*.

Any irreducible polynomial over GF(2) of degree *m* divides $X^{2^m-1}+1$.

An irreducible polynomial $p(X)$ of degree *m* is said to be *primitive* if the smallest positive integer *n* for which $p(X)$ divides X^n+1 is *n* = 2^m – 1.

Polynomials over GF(2) may be irreducible but not primitive. It is not easy to recognize primitive polynomials. There are tables of irreducible polynomials that indicate which of these polynomials are also primitive. For a given degree *m* there may be more than one primitive polynomial.

Polynomial Calculations Over GF(2)

Suppose we have two polynomials in X over GF(2):

$$m(X)=1+X+X^3$$
$$g(X)=1+X^4$$

Represented as binary sequences with the polynomial coefficients in ascending order:

$$m=[1101]$$
$$g=[10001]$$

Now compute:

$$c(X)=X^3m(X)=X^3+X^4+X^6$$

Divide $c(X)$ by $g(X)$:

$$\begin{array}{l}
\qquad\qquad X^2+1=q(X)\\
X^4+1\;\overline{\left)X^6+X^4+X^3\right.}\\
\qquad\qquad X^6 \qquad\qquad +X^2\\
\hline
\qquad\qquad X^4+X^3+X^2\\
\qquad\qquad X^4 \qquad\qquad +1\\
\hline
\qquad\qquad\qquad X^3+X^2+1=r(X)
\end{array}$$

So $c(X)=q(X)g(X)+r(X)$ using the form of Euclid’s division algorithm.

Check:

$$c(X)=(X^2+1)(X^4+1)+(X\text{¿¿}3+X^2+1)\text{¿}$$

$$\text{¿}X^6+X^4+X^2+1+X^3+X^2+1$$

$$\text{¿}X^6+X^4+X^3$$

The MATLAB functions `gfconv` and `gfdeconv` perform polynomial multiplication and division over GF(2). They assume the binary sequences representing the polynomial coefficients are in *ascending* order.

```
>> M = [1 1 0 1]

M =

     1     1     0     1

>> G = [1 0 0 0 1]

G =

     1     0     0     0     1

>> X3 = [0 0 0 1]

X3 =

     0     0     0     1


>> C = gfconv(X3, M)

C =

     0     0     0     1     1     0     1


>> [Q, R] = gfdeconv(C, G)

Q =

     1     0     1

R =

     1     0     1     1
```

The degree 3 polynomial $p(X)$ below is primitive:

$$p(X)=1+X+X^3$$

It divides X^7+1 with no remainder:

$$
\begin{array}{rl}
 & X^4+X^2+X+1 \\ \cline{2-2}
X^3+X+1\ X^7 & \Big| \qquad\qquad\qquad\qquad +1 \\
 & X^7+X^5+X^4 \\ \cline{2-2}
 & \quad X^5+X^4 \qquad\qquad\qquad +1 \\
 & \quad X^5 \qquad +X^3+X^2 \\ \cline{2-2}
 & \qquad X^4+X^3+X^2 \qquad +1 \\
 & \qquad X^4 \qquad +X^2+X \\ \cline{2-2}
 & \qquad\quad X^3 \qquad +X+1 \\
 & \qquad\quad X^3 \qquad +X+1 \\ \cline{2-2}
 & \qquad\qquad\qquad\qquad 0
\end{array}
$$

Verify using MATLAB

```
>> [Q, R] = gfdeconv([1 0 0 0 0 0 0 1], [1 1 0 1])

Q =

     1     1     1     0     1

R =

     0
```

The MATLAB functions `gfconv` and `gfdeconv` are so named because polynomial multiplication and division are equivalent respectively to the discrete convolution and deconvolution of sequences representing the polynomial coefficients.

Construction of GF(2^m)

The Galois extension field GF(2^m) with 2^m elements where m > 1 can be constructed from GF(2).

Start with the two elements 0 and 1 from GF(2) and add a new element α. Extend modulo-2 multiplication to introduce a sequence of powers of α:

$\alpha^0 = 1$

$\alpha^1 = \alpha$

$\alpha^2 = \alpha \cdot \alpha$

$\alpha^3 = \alpha \cdot \alpha \cdot \alpha$

$\alpha^j = \alpha \cdot \alpha \cdot \ldots \cdot \alpha \quad (\text{j times})$

The infinite set $F = \{0, 1, \alpha, \alpha^2, \ldots, \alpha^j, \ldots\}$ now has a defined multiplication operation.

Require that α be a root of a primitive polynomial $p(X)$ of degree *m* over GF(2). Then $p(\alpha)$ = 0 and $p(X)$ divides $X^{2^m-1}+1$:

$X^{2^m-1}+1 = q(X)\,p(X)$

$\alpha^{2^m-1}+1 = q(\alpha)\,p(\alpha)$

$\alpha^{2^m-1}+1 = q(\alpha) \cdot 0$

$\alpha^{2^m-1} = 1$

The set F then becomes finite with 2^m elements: $F^{¿} = \{0, 1, \alpha, \alpha^2, \ldots, \alpha^{2^m-2}\}$.

The multiplicative inverse of α^i is α^{2^m-1-i} for 0 < *i* < 2^m – 1.

The nonzero elements of $F^{¿}$ form a cyclic commutative group under this definition of multiplication.

In addition to powers of α the nonzero elements of $F^{¿}$ can also be represented by polynomials. For 0 ≤ *i* < 2^m – 1 divide X^i by the primitive polynomial $p(X)$ of degree *m*:

$$X^i = q_i(X)\,p(X) + r_i(X)$$

The remainder $r_i(X)$ is a polynomial of degree *m* – 1 or less over GF(2) of the form:

$$r_i(X) = r_{i0} + r_{i1}X + r_{i2}X^2 + \ldots + r_{i,m-1}X^{m-1}$$

Because $p(X)$ is primitive and hence irreducible, X and $p(X)$ are relatively prime. X^i is therefore not divisible by $p(X)$ thus $r_i(X)$ ≠ 0 for each *i*. It can be shown that these 2^m nonzero $r_i(X)$ are distinct.

Now for *i* = 0, 1, 2, ..., 2^m – 2, replace X with α in the expression for X^i above. Since α is a root of $p(X)$, $q_i(\alpha)\,p(\alpha) = q_i(\alpha)\cdot 0 = 0$. Therefore:

$$\alpha^i = r_i(\alpha) = r_{i0} + r_{i1}\alpha + r_{i2}\alpha^2 + \ldots + r_{i,m-1}\alpha^{m-1}$$

The 2^m – 1 nonzero elements of $F^{¿}$ are now represented by 2^m – 1 distinct nonzero polynomials of α over GF(2) with degree m – 1 or less. The zero element in $F^{¿}$ can be represented by the zero polynomial. As a result, the 2^m elements of $F^{¿}$ are represented by 2^m distinct polynomials of α over GF(2).

Extend modulo-2 addition to include the powers of α:

$$0 + \alpha^i = \alpha^i + 0$$

Add the polynomial representations of the elements in $F^{¿}$ using modulo-2 addition to determine the various coefficients.

The additive inverse of any element in $F^{¿}$ is itself since $\alpha^i + \alpha^i = (1+1)\alpha^i = 0$.

The elements of $F^{¿}$ form a commutative group under this definition of addition.

Finally, multiplication on $F^{¿}$ is distributive over addition on $F^{¿}$. The set $F^{¿}$ is therefore a Galois field of 2^m elements. Since the addition and multiplication operations defined on $F^{¿}$ = GF(2^m) imply modulo-2 addition and multiplication, GF(2) forms a subfield of GF(2^m). GF(2) is called the *ground field* of GF(2^m). The characteristic of GF(2^m) is 2.

As an example we construct GF(2^3) = GF(8) using the primitive polynomial:

$$p(X) = 1 + X + X^3$$

GF(8) begins with the two elements from GF(2), namely 0 and 1. The next element is α which must be a root of $p(X)$:

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

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

Next we find: $\alpha^4=\alpha\cdot\alpha^3=\alpha(1+\alpha)=\alpha+\alpha^2$

$$\alpha^5=\alpha\cdot\alpha^4=\alpha(\alpha+\alpha^2)=\alpha^2+\alpha^3=1+\alpha+\alpha^2$$

$$\alpha^6=\alpha\cdot\alpha^5=\alpha(1+\alpha+\alpha^2)=\alpha+\alpha^2+\alpha^3=1+\alpha^2$$

Because $p(X)$ is primitive it must divide $X^{2^3-1}+1=X^7+1$ evenly:

$$X^7+1=q(X)\,p(X)$$

$$\alpha^7+1=q(\alpha)\,p(\alpha)$$

$$\alpha^7+1=q(\alpha)\cdot 0$$

$$\alpha^7=1$$

The complete field GF(8) with the primitive polynomial $p(X)=1+X+X^3$ is:

0
1
α
α^2
$\alpha^3=1+\alpha$
$\alpha^4=\alpha+\alpha^2$
$\alpha^5=1+\alpha+\alpha^2$
$\alpha^6=1+\alpha^2$

When performing calculations in an extension field the polynomial forms of the various elements are used for addition and subtraction while the exponential forms are used for multiplication and division.

These examples are over GF(8) with $p(X)=1+X+X^3$:

$$\alpha^3+\alpha^4=(1+\alpha)+(\alpha+a^2)=1+\alpha^2=\alpha^6$$

$$\alpha^6-\alpha^4=(1+\alpha^2)-(\alpha+a^2)=1-\alpha=1+\alpha=\alpha^3$$

$$\alpha^4\cdot\alpha^5=\alpha^9=\alpha^2\cdot\alpha^7=\alpha^2\cdot 1=\alpha^2$$

$$\alpha^4/\alpha^5=\alpha^4\cdot\alpha^{7-5}=\alpha^4\cdot\alpha^2=\alpha^6$$

$$g(X)=(X+\alpha)(X+\alpha¿¿2)=\alpha^3+(\alpha+\alpha^2)X+X^2¿$$

$$¿\alpha^3+\alpha^4X+X^2$$

Complete addition and multiplication tables for an extension field can be constructed to facilitate these types of calculations.

Applications like MATLAB can perform mathematical operations over extension fields. They make use of binary n-tuple or decimal representations for the polynomial forms of the field elements. Using the little-endian convention for GF(8) the following table can be constructed:

Exponential	**Polynomial**	**3-tuple**	**Decimal**
0	0	[0 0 0]	0
1	1	[1 0 0]	1
α	α	[0 1 0]	2
α^2	α^2	[0 0 1]	4
α^3	$1+\alpha$	[1 1 0]	3
α^4	$\alpha+\alpha^2$	[0 1 1]	6
α^5	$1+\alpha+\alpha^2$	[1 1 1]	7
α^6	$1+\alpha^2$	[1 0 1]	5

Revisiting the examples above first define the element α with the `gf` function:

```
>> alpha = gf(2, 3)

alpha = GF(2^3) array. Primitive polynomial = D^3+D+1 (11
decimal)

Array elements =

   2
```

Next use the array `A` for the field elements $\alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6$:

```
>> A = gf(alpha.^(1:6), 3)

A = GF(2^3) array. Primitive polynomial = D^3+D+1 (11 decimal)

Array elements =

   2   4   3   6   7   5
```

$\alpha^3+\alpha^4=\alpha^6$

```
>> A(3) + A(4)

ans = GF(2^3) array. Primitive polynomial = D^3+D+1 (11 decimal)

Array elements =

   5
```

$\alpha^6-\alpha^4=\alpha^3$

```
>> A(6) - A(4)

ans = GF(2^3) array. Primitive polynomial = D^3+D+1 (11 decimal)

Array elements =

   3
```

$\alpha^4 \cdot \alpha^5 = \alpha^2$

```
>> A(4) * A(5)

ans = GF(2^3) array. Primitive polynomial = D^3+D+1 (11 decimal)

Array elements =

   4
```

$\alpha^4 / \alpha^5 = \alpha^6$

```
>> A(4) / A(5)

ans = GF(2^3) array. Primitive polynomial = D^3+D+1 (11 decimal)

Array elements =

   5
```

$g(X)=(X+\alpha)(X+\alpha$¿¿$2)=\alpha^3+\alpha^4 X+X^2$¿

```
>> G = conv([1 A(1)], [1 A(2)])

G = GF(2^3) array. Primitive polynomial = D^3+D+1 (11 decimal)

Array elements =

   1   6   3
```

Note that unlike `gfconv` and `gfdeconv` which assume the polynomial coefficients are in ascending order, `conv` and `deconv` assume the polynomial coefficients are in *descending* order.

The roots of $g(X)$ can be found with the `roots` function:

```
>> roots(G)

ans = GF(2^3) array. Primitive polynomial = D^3+D+1 (11 decimal)

Array elements =

   2
   4
```

Recall that the parity array matrix A for the Golay(24,12) code has the following properties:

$A = A^T$

$A A^T = I$

From which we can conclude: $A = A^{-1}$

MATLAB will give an unexpected result if A is defined over the infinite field of real numbers:

```
>> A

A =

     1     1     0     1     1     1     0     0     0     1     0     1
     1     0     1     1     1     0     0     0     1     0     1     1
     0     1     1     1     0     0     0     1     0     1     1     1
     1     1     1     0     0     0     1     0     1     1     0     1
     1     1     0     0     0     1     0     1     1     0     1     1
     1     0     0     0     1     0     1     1     0     1     1     1
     0     0     0     1     0     1     1     0     1     1     1     1
     0     0     1     0     1     1     0     1     1     1     0     1
     0     1     0     1     1     0     1     1     1     0     0     1
     1     0     1     1     0     1     1     1     0     0     0     1
     0     1     1     0     1     1     1     0     0     0     1     1
     1     1     1     1     1     1     1     1     1     1     1     0

>> inv(A)

ans =

    0.1515    0.1515   -0.1818    0.1515    0.1515    0.1515   -0.1818   -0.1818   -0.1818    0.1515   -0.1818
0.0909
    0.1515   -0.1818    0.1515    0.1515    0.1515   -0.1818   -0.1818   -0.1818    0.1515   -0.1818    0.1515
0.0909
   -0.1818    0.1515    0.1515    0.1515   -0.1818   -0.1818   -0.1818    0.1515   -0.1818    0.1515    0.1515
0.0909
    0.1515    0.1515    0.1515   -0.1818   -0.1818   -0.1818    0.1515   -0.1818    0.1515    0.1515   -0.1818
0.0909
    0.1515    0.1515   -0.1818   -0.1818   -0.1818    0.1515   -0.1818    0.1515    0.1515   -0.1818    0.1515
0.0909
    0.1515   -0.1818   -0.1818   -0.1818    0.1515   -0.1818    0.1515    0.1515   -0.1818    0.1515    0.1515
0.0909
```

```
   -0.1818   -0.1818   -0.1818    0.1515   -0.1818    0.1515    0.1515   -0.1818    0.1515    0.1515    0.1515
0.0909
   -0.1818   -0.1818    0.1515   -0.1818    0.1515    0.1515   -0.1818    0.1515    0.1515    0.1515   -0.1818
0.0909
   -0.1818    0.1515   -0.1818    0.1515    0.1515   -0.1818    0.1515    0.1515    0.1515   -0.1818   -0.1818
0.0909
    0.1515   -0.1818    0.1515    0.1515   -0.1818    0.1515    0.1515    0.1515   -0.1818   -0.1818   -0.1818
0.0909
   -0.1818    0.1515    0.1515   -0.1818    0.1515    0.1515    0.1515   -0.1818   -0.1818   -0.1818    0.1515
0.0909
    0.0909    0.0909    0.0909    0.0909    0.0909    0.0909    0.0909    0.0909    0.0909    0.0909    0.0909   -
0.5455
```

However if a new matrix Z is created which is the elements of A defined over GF(2) then we get the expected result.

```
>> Z = gf(A, 1)

Z = GF(2) array.

Array elements =

   1   1   0   1   1   1   0   0   0   1   0   1
   1   0   1   1   1   0   0   0   1   0   1   1
   0   1   1   1   0   0   0   1   0   1   1   1
   1   1   1   0   0   0   1   0   1   1   0   1
   1   1   0   0   0   1   0   1   1   0   1   1
   1   0   0   0   1   0   1   1   0   1   1   1
   0   0   0   1   0   1   1   0   1   1   1   1
   0   0   1   0   1   1   0   1   1   1   0   1
   0   1   0   1   1   0   1   1   1   0   0   1
   1   0   1   1   0   1   1   1   0   0   0   1
   0   1   1   0   1   1   1   0   0   0   1   1
   1   1   1   1   1   1   1   1   1   1   1   0



>> inv(Z)

ans = GF(2) array.

Array elements =

   1   1   0   1   1   1   0   0   0   1   0   1
   1   0   1   1   1   0   0   0   1   0   1   1
   0   1   1   1   0   0   0   1   0   1   1   1
   1   1   1   0   0   0   1   0   1   1   0   1
```

```
1   1   0   0   0   1   0   1   1   0   1   1
1   0   0   0   1   0   1   1   0   1   1   1
0   0   0   1   0   1   1   0   1   1   1   1
0   0   1   0   1   1   0   1   1   1   0   1
0   1   0   1   1   0   1   1   1   0   0   1
1   0   1   1   0   1   1   1   0   0   0   1
0   1   1   0   1   1   1   0   0   0   1   1
1   1   1   1   1   1   1   1   1   1   1   0
```

```
>> Z * inv(Z)

ans = GF(2) array.

Array elements =

   1   0   0   0   0   0   0   0   0   0   0   0
   0   1   0   0   0   0   0   0   0   0   0   0
   0   0   1   0   0   0   0   0   0   0   0   0
   0   0   0   1   0   0   0   0   0   0   0   0
   0   0   0   0   1   0   0   0   0   0   0   0
   0   0   0   0   0   1   0   0   0   0   0   0
   0   0   0   0   0   0   1   0   0   0   0   0
   0   0   0   0   0   0   0   1   0   0   0   0
   0   0   0   0   0   0   0   0   1   0   0   0
   0   0   0   0   0   0   0   0   0   1   0   0
   0   0   0   0   0   0   0   0   0   0   1   0
   0   0   0   0   0   0   0   0   0   0   0   1
```

Properties of GF(2^m)

A useful property of polynomials over GF(2) is:

$[f(X)]^{2^k} = f\left(X^{2^k}\right)$ for any $k \geq 0$

A polynomial over GF(2) may not have roots from GF(2) but from an extension field GF(2^m).

Suppose $f(X)$ is a polynomial over GF(2) and β is an element from an extension field GF(2^m). If β is a root of $f(X)$ then β^{2^k} is also a root of $f(X)$ for any $k \geq 0$. The element β^{2^k} is called a *conjugate* of β.

The 2^m – 1 nonzero elements of GF(2^m) form all the roots of $X^{2^m-1}+1$. Including the zero element, the 2^m elements of GF(2^m) form all the roots of $X^{2^m}+X$.

Let $\phi(X)$ be the polynomial of smallest degree over GF(2) such that $\phi(\beta)=0$. This unique polynomial is called the *minimal polynomial* of β.

The minimal polynomial $\phi(X)$ of a field element β is irreducible.

Let $f(X)$ be a polynomial over GF(2) and $\phi(X)$ be the minimal polynomial of a field element β. If β is a root of $f(X)$ then $f(X)$ is divisible by $\phi(X)$.

GF(4)

```
Generator Polynomial:
   p(X) = 1 + X + X^2


Elements:
   Power      Polynomial       2-Tuple     Decimal
   0          0                [0  0]            0
   1          1                [1  0]            1
   α              α            [0  1]            2
   α^2        1 + α            [1  1]            3


Minimal Polynomials and Conjugate Roots:
   φ1(X) = 1 + X + X^2
   α, α^2
```

GF(8)

```
Generator Polynomial:
   p(X) = 1 + X + X^3


Elements:
   Power      Polynomial       3-Tuple     Decimal
   0          0                [0  0  0]         0
   1          1                [1  0  0]         1
   α              α            [0  1  0]         2
   α^2                α^2      [0  0  1]         4
   α^3        1 + α            [1  1  0]         3
   α^4            α + α^2      [0  1  1]         6
   α^5        1 + α + α^2      [1  1  1]         7
   α^6        1     + α^2      [1  0  1]         5


Minimal Polynomials and Conjugate Roots:
   φ1(X) = 1 + X + X^3
   α, α^2, α^4

   φ3(X) = 1 + X^2 + X^3
   α^3, α^5, α^6
```

GF(16)

```
Generator Polynomial:
   p(X) = 1 + X + X^4


Elements:
   Power      Polynomial             4-Tuple        Decimal
   0          0                      [0  0  0  0]         0
   1          1                      [1  0  0  0]         1
   α              α                  [0  1  0  0]         2
   α^2                α^2            [0  0  1  0]         4
   α^3                      α^3      [0  0  0  1]         8
   α^4        1 + α                  [1  1  0  0]         3
   α^5            α + α^2            [0  1  1  0]         6
   α^6                α^2 + α^3      [0  0  1  1]        12
   α^7        1 + α       + α^3      [1  1  0  1]        11
   α^8        1     + α^2            [1  0  1  0]         5
   α^9            α       + α^3      [0  1  0  1]        10
   α^10       1 + α + α^2            [1  1  1  0]         7
   α^11           α + α^2 + α^3      [0  1  1  1]        14
   α^12       1 + α + α^2 + α^3      [1  1  1  1]        15
   α^13       1     + α^2 + α^3      [1  0  1  1]        13
   α^14       1           + α^3      [1  0  0  1]         9


Minimal Polynomials and Conjugate Roots:
   φ1(X) = 1 + X + X^4
   α, α^2, α^4, α^8

   φ3(X) = 1 + X + X^2 + X^3 + X^4
   α^3, α^6, α^9, α^12

   φ5(X) = 1 + X + X^2
   α^5, α^10

   φ7(X) = 1 + X^3 + X^4
   α^7, α^11, α^13, α^14
```

GF(32)

```
Generator Polynomial:
   p(X) = 1 + X^2 + X^5


Elements:
   Power      Polynomial                   5-Tuple
Decimal
   0          0                            [0  0  0  0  0]
0
   1          1                            [1  0  0  0  0]
1
   α              α                        [0  1  0  0  0]
2
   α^2                α^2                  [0  0  1  0  0]
4
   α^3                      α^3            [0  0  0  1  0]
8
   α^4                            α^4      [0  0  0  0  1]
16
   α^5        1     + α^2                  [1  0  1  0  0]
5
   α^6            α       + α^3            [0  1  0  1  0]
10
   α^7                α^2       + α^4      [0  0  1  0  1]
20
   α^8        1     + α^2 + α^3            [1  0  1  1  0]
13
   α^9            α       + α^3 + α^4      [0  1  0  1  1]
26
   α^10       1                 + α^4      [1  0  0  0  1]
17
   α^11       1 + α + α^2                  [1  1  1  0  0]
7
   α^12           α + α^2 + α^3            [0  1  1  1  0]
14
   α^13               α^2 + α^3 + α^4      [0  0  1  1  1]
28
   α^14       1     + α^2 + α^3 + α^4      [1  0  1  1  1]
29
   α^15       1 + α + α^2 + α^3 + α^4      [1  1  1  1  1]
31
   α^16       1 + α       + α^3 + α^4      [1  1  0  1  1]
27
   α^17       1 + α             + α^4      [1  1  0  0  1]
19
   α^18       1 + α                        [1  1  0  0  0]
3
```

```
   α^19           α + α^2                  [0  1  1  0  0]
6
   α^20               α^2 + α^3            [0  0  1  1  0]
12
   α^21                     α^3 + α^4      [0  0  0  1  1]
24
   α^22       1     + α^2       + α^4      [1  0  1  0  1]
21
   α^23       1 + α + α^2 + α^3            [1  1  1  1  0]
15
   α^24           α + α^2 + α^3 + α^4      [0  1  1  1  1]
30
   α^25       1           + α^3 + α^4      [1  0  0  1  1]
25
   α^26       1 + α + α^2       + α^4      [1  1  1  0  1]
23
   α^27       1 + α       + α^3            [1  1  0  1  0]
11
   α^28           α + α^2       + α^4      [0  1  1  0  1]
22
   α^29       1           + α^3            [1  0  0  1  0]
9
   α^30           α             + α^4      [0  1  0  0  1]
18
```

```
Minimal Polynomials and Conjugate Roots:
   φ1(X) = 1 + X^2 + X^5
   α, α^2, α^4, α^8, α^16

   φ3(X) = 1 + X^2 + X^3 + X^4 + X^5
   α^3, α^6, α^12, α^17, α^24

   φ5(X) = 1 + X + X^2 + X^4 + X^5
   α^5, α^9, α^10, α^18, α^20

   φ7(X) = 1 + X + X^2 + X^3 + X^5
   α^7, α^14, α^19, α^25, α^28

   φ11(X) = 1 + X + X^3 + X^4 + X^5
   α^11, α^13, α^21, α^22, α^26

   φ15(X) = 1 + X^3 + X^5
   α^15, α^23, α^27, α^29, α^30
```

GF(64)

```
Generator Polynomial:
   p(X) = 1 + X + X^6


Elements:
   Power      Polynomial                         6-Tuple
Decimal
   0          0                                  [0  0  0  0  0  0]
0
   1          1                                  [1  0  0  0  0  0]
1
   α              α                              [0  1  0  0  0  0]
2
   α^2                α^2                        [0  0  1  0  0  0]
4
   α^3                      α^3                  [0  0  0  1  0  0]
8
   α^4                            α^4            [0  0  0  0  1  0]
16
   α^5                                  α^5      [0  0  0  0  0  1]
32
   α^6        1 + α                              [1  1  0  0  0  0]
3
   α^7            α + α^2                        [0  1  1  0  0  0]
6
   α^8                α^2 + α^3                  [0  0  1  1  0  0]
12
   α^9                      α^3 + α^4            [0  0  0  1  1  0]
24
   α^10                           α^4 + α^5      [0  0  0  0  1  1]
48
   α^11       1 + α                   + α^5      [1  1  0  0  0  1]
35
   α^12       1     + α^2                        [1  0  1  0  0  0]
5
   α^13           α       + α^3                  [0  1  0  1  0  0]
10
   α^14               α^2       + α^4            [0  0  1  0  1  0]
20
   α^15                     α^3       + α^5      [0  0  0  1  0  1]
40
   α^16       1 + α             + α^4            [1  1  0  0  1  0]
19
   α^17           α + α^2             + α^5      [0  1  1  0  0  1]
38
   α^18       1 + α + α^2 + α^3                  [1  1  1  1  0  0]
15
```

```
   α^19           α + α^2 + α^3 + α^4            [0  1  1  1  1  0]
30
   α^20               α^2 + α^3 + α^4 + α^5      [0  0  1  1  1  1]
60
   α^21       1 + α       + α^3 + α^4 + α^5      [1  1  0  1  1  1]
59
   α^22       1     + α^2       + α^4 + α^5      [1  0  1  0  1  1]
53
   α^23       1           + α^3       + α^5      [1  0  0  1  0  1]
41
   α^24       1                 + α^4            [1  0  0  0  1  0]
17
   α^25           α                   + α^5      [0  1  0  0  0  1]
34
   α^26       1 + α + α^2                        [1  1  1  0  0  0]
7
   α^27           α + α^2 + α^3                  [0  1  1  1  0  0]
14
   α^28               α^2 + α^3 + α^4            [0  0  1  1  1  0]
28
   α^29                     α^3 + α^4 + α^5      [0  0  0  1  1  1]
56
   α^30       1 + α             + α^4 + α^5      [1  1  0  0  1  1]
51
   α^31       1     + α^2             + α^5      [1  0  1  0  0  1]
37
   α^32       1           + α^3                  [1  0  0  1  0  0]
9
   α^33           α             + α^4            [0  1  0  0  1  0]
18
   α^34               α^2             + α^5      [0  0  1  0  0  1]
36
   α^35       1 + α       + α^3                  [1  1  0  1  0  0]
11
   α^36           α + α^2       + α^4            [0  1  1  0  1  0]
22
   α^37               α^2 + α^3       + α^5      [0  0  1  1  0  1]
44
   α^38       1 + α       + α^3 + α^4            [1  1  0  1  1  0]
27
   α^39           α + α^2       + α^4 + α^5      [0  1  1  0  1  1]
54
   α^40       1 + α + α^2 + α^3       + α^5      [1  1  1  1  0  1]
47
   α^41       1     + α^2 + α^3 + α^4            [1  0  1  1  1  0]
29
   α^42           α       + α^3 + α^4 + α^5      [0  1  0  1  1  1]
58
   α^43       1 + α + α^2       + α^4 + α^5      [1  1  1  0  1  1]
55
```

```
   α^44       1     + α^2 + α^3       + α^5      [1  0  1  1  0  1]
45
   α^45       1           + α^3 + α^4            [1  0  0  1  1  0]
25
   α^46           α             + α^4 + α^5      [0  1  0  0  1  1]
50
   α^47       1 + α + α^2             + α^5      [1  1  1  0  0  1]
39
   α^48       1     + α^2 + α^3                  [1  0  1  1  0  0]
13
   α^49           α       + α^3 + α^4            [0  1  0  1  1  0]
26
   α^50               α^2       + α^4 + α^5      [0  0  1  0  1  1]
52
   α^51       1 + α       + α^3       + α^5      [1  1  0  1  0  1]
43
   α^52       1     + α^2       + α^4            [1  0  1  0  1  0]
21
   α^53           α       + α^3       + α^5      [0  1  0  1  0  1]
42
   α^54       1 + α + α^2       + α^4            [1  1  1  0  1  0]
23
   α^55           α + α^2 + α^3       + α^5      [0  1  1  1  0  1]
46
   α^56       1 + α + α^2 + α^3 + α^4            [1  1  1  1  1  0]
31
   α^57           α + α^2 + α^3 + α^4 + α^5      [0  1  1  1  1  1]
62
   α^58       1 + α + α^2 + α^3 + α^4 + α^5      [1  1  1  1  1  1]
63
   α^59       1     + α^2 + α^3 + α^4 + α^5      [1  0  1  1  1  1]
61
   α^60       1           + α^3 + α^4 + α^5      [1  0  0  1  1  1]
57
   α^61       1                 + α^4 + α^5      [1  0  0  0  1  1]
49
   α^62       1                       + α^5      [1  0  0  0  0  1]
33
```

```
Minimal Polynomials and Conjugate Roots:
   φ1(X) = 1 + X + X^6
   α, α^2, α^4, α^8, α^16, α^32

   φ3(X) = 1 + X + X^2 + X^4 + X^6
   α^3, α^6, α^12, α^24, α^33, α^48

   φ5(X) = 1 + X + X^2 + X^5 + X^6
   α^5, α^10, α^17, α^20, α^34, α^40

   φ7(X) = 1 + X^3 + X^6
   α^7, α^14, α^28, α^35, α^49, α^56

   φ9(X) = 1 + X^2 + X^3
   α^9, α^18, α^36

   φ11(X) = 1 + X^2 + X^3 + X^5 + X^6
   α^11, α^22, α^25, α^37, α^44, α^50

   φ13(X) = 1 + X + X^3 + X^4 + X^6
   α^13, α^19, α^26, α^38, α^41, α^52

   φ15(X) = 1 + X^2 + X^4 + X^5 + X^6
   α^15, α^30, α^39, α^51, α^57, α^60

   φ21(X) = 1 + X + X^2
   α^21, α^42

   φ23(X) = 1 + X + X^4 + X^5 + X^6
   α^23, α^29, α^43, α^46, α^53, α^58

   φ27(X) = 1 + X + X^3
   α^27, α^45, α^54

   φ31(X) = 1 + X^5 + X^6
   α^31, α^47, α^55, α^59, α^61, α^62
```