Abstract Algebra for Cryptography Part I

Algebraic Properties and Field Arihmetic

Izmir Institute of Technology

Department of Computer Engineering

Asst. Prof. Serap ŞAHİN

2011

Outline

- Algebraic Properties
  - Basic concepts in Set theory
  - The random mappings
  - Groups
  - Cyclic Groups
  - Generators
  - Rings
  - Fields
- Field Arithmetic
  - Prime Field Arithmetic
  - Binary Field (Polynomial) Arithmetic

Concepts in Set Theory

Set → *A* collection of well defined elements.

1. **Description** – ***A* set defined in words.**
   - **Example**: Set *A* is the set of Natural numbers ending in 10.
2. **Roster** – *A* set is defined with a list of elements surrounded by braces { }.
   - **Example:** $A = \{1,2,3,4,5,6,7,8,9,10\}$
3. **Set Builder Notation**
   - **Example: $A = \{x | x$ is a natural number less than 11}**, which reads: "Set *A* is set of all elements x such that x is a natural number less than 11."

Concepts in Set Theory

- **Element** → **An item in a set denoted by the symbol ∈.**
  - Example: If $A = \{1,2,3\}$, then $3 \in A$
- **Equal sets** → **are identical, containing exactly the same elements.**
  - Example: If $A = \{A,B,C,D\}$, and $B = \{D,C,B,A\}$, then $A = B$
- **Equivalent sets** → **have the same cardinal number of elements, denoted by the symbol n( ), but the elements do not need to be identical.**
  - Example: If $A = \{1,2,3,4\}$ and $B = \{$April, May, June, July$\}$, then $n(A)=n(B)$. Sets A and B are equivalent.

Concepts in Set Theory

- **Empty or Null Set** → is a set that contains no elements and are denoted by the symbols { } and ∅.
- **Subset** → denoted by the symbol ⊆ occurs when all the elements of one set are also the elements of another. A subset may be, but doesn't have to be equal to the original set.
  - Example: If A = {A,B,C,D} and B = {A,B,C,D,E,F,G}, then A ⊆ B.
- **Proper Subset** → denoted by the symbol ⊂ occurs when the subset contains at least one less element than the original set.
  - Example: If A = {A,B,C,D} and B = {A,B,D}, then B ⊂ A

Concepts in Set Theory

- **Number of Subsets** → is 2^n , where n is the number of elements in the set.
  - Example: A = {A, B, C, D}. Since set A has 4 elements, the formula for number of subsets is: $2^4 = 16$.
  - Therefore, there are 16 subsets of set A. They are: ∅, {A}, {B}, {C}, {D}, {A,B}, {A,C}, {A,D}, {B,C}, {B,D}, {C,D}, {A,B,C}, {A,B,D}, {A,C,D}, {B,C,D} and {A,B,C,D}.
  - Note that the first fifteen subsets of set A are also **proper subsets**. The formula for the number of proper subsets is $2^n - 1$. In this example of set A, the number of proper subsets is $2^4 - 1 = 15$.

Concepts in Set Theory

- **Universal Set** → contains all the elements for any specific discussion, and is symbolized by the symbol **U**.
  - Example: **U = {A,E,I,O,U}**
- **Intersection** → contains the elements common to 2 or more sets and is denoted by the symbol, ∩.
- **Union** → contains all the elements in two or more sets and is denoted by the symbol, ∪.
- **Complement** → contains all the elements in the universal set that are not in the original set and is denoted by the symbol, ′ or ¯.
  - Example: U = {1,2,3,4,5,6,7,8,9,0} A= {1,2,3,} B = {2,3,4,5,6}
  - A ∩ B = {2,3}, A ∪ B = {1,2,3,4,5,6}, A′ = {4,5,6,7,8,9,0} B′={1,7,8,9,0}

The Random Mappings

Definition:

Let F_n denote **the collection of all functions (mappings)** from a finite domain of size n to a finite codomain of size n.

Models where random elements of F_n are considered are called *random mappings models*.

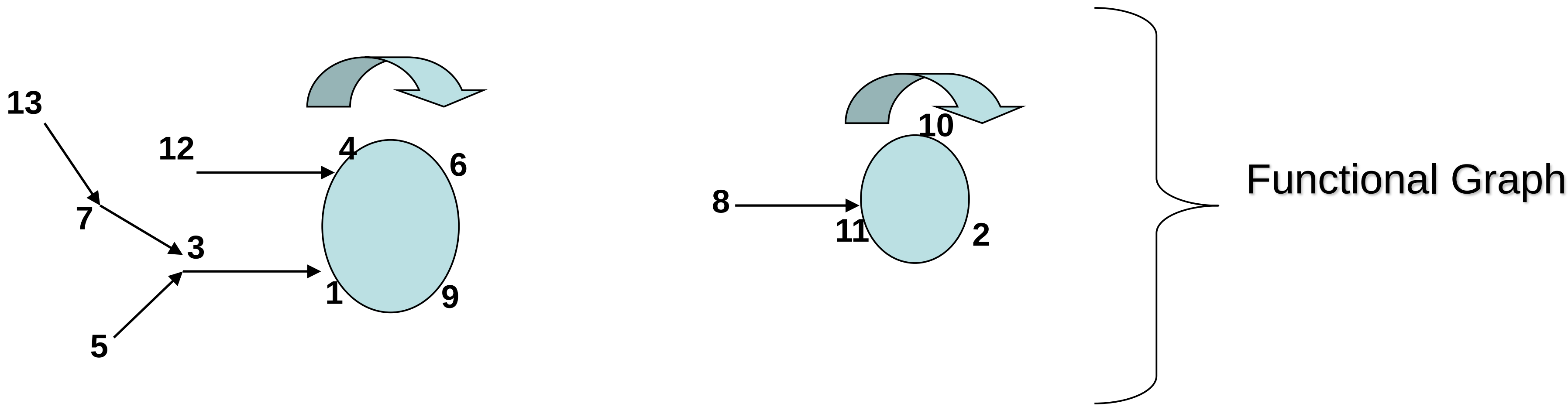
Definition:

Let f be a function in F_n with domain and codomain equal to {1,2,..,n}. The ***functional graph*** of f is a **directed graph** whose ***points*** are the elements {1,2,..,n} and whose ***edges*** are the ordered pairs (x, f(x)) for all x ϵ {1,2,..,n}.

Example: The Random Mappings

Consider the function f:{1,2,..,13}→{1,2,..,13} defined by following table:

f(1)=4	f(2)=11	f(3)=1	f(4)=6	f(5)=3	f(6)=9	f(7)=3	f(8)=11	f(9)=1	f(10)=2	f(11)=10	f(12)=4	f(13)=7



Definition Let f be a random function from $\{1, 2, \ldots, n\}$ to $\{1, 2, \ldots, n\}$ and let $u \in \{1, 2, \ldots, n\}$. Consider the sequence of points $u_0, u_1, u_2, \ldots$ defined by $u_0 = u$, $u_i = f(u_{i-1})$ for $i \geq 1$. In terms of the functional graph of f, this sequence describes a path that connects to a cycle.

(i) The number of edges in the path is called the *tail length* of u, denoted $\lambda(u)$.

(ii) The number of edges in the cycle is called the *cycle length* of u, denoted $\mu(u)$.

(iii) The *rho-length* of u is the quantity $\rho(u) = \lambda(u) + \mu(u)$.

Example The functional graph in Figure 2.1 has 2 components and 4 terminal points. The point $u = 3$ has parameters $\lambda(u) = 1$, $\mu(u) = 4$, $\rho(u) = 5$. The tree, component, and predecessors sizes of $u = 3$ are 4, 9, and 3, respectively. □

The Groups

- A group (G, .) is a set of elements G with binary operations "." that satisfy the following axioms for x, y in G:
  - Closure : x.y is in G.
  - Associativity : x.(y.z) = (x.y).z
  - There exists an identity element *e* in G such that for all *x* in G:

    (x.e) = (e.x) = x
  - There exists an inverse x^{-1} in G such that

    $(x.x^{-1}) = (x^{-1}.x) = e$ for all x in G.

    Example: (Z, +) is a group
  - A group that is commutative is also known as *abelian: x.y = y.x*

Cyclic Group and Generator

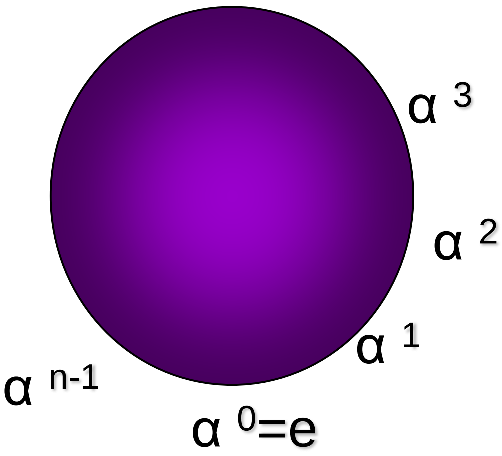
- Let G is a group and $a \in G$
- If $G=\{a^n \mid n \in Z\}$, then a is a generator of G and the group

  $G=\langle a \rangle$ is cyclic.
- If the cyclic group $\langle a \rangle$ of G is finite, then the order of a is the $|\langle a \rangle|$ of this cyclic subgroup. Otherwise, we say that G has infinite order.
- If $a \in G$ is finite order m, than m is the smallest positive integer such that $a^m=e$.
- Every cyclic group is abelian. (commutative axiom)
- A subgroup of a cyclic group is cyclic.

Cyclic Groups

1. If <G> has an <u>infinite</u> number of elements, then there is no two distinct exponents h and k which can point to the same element in the group.

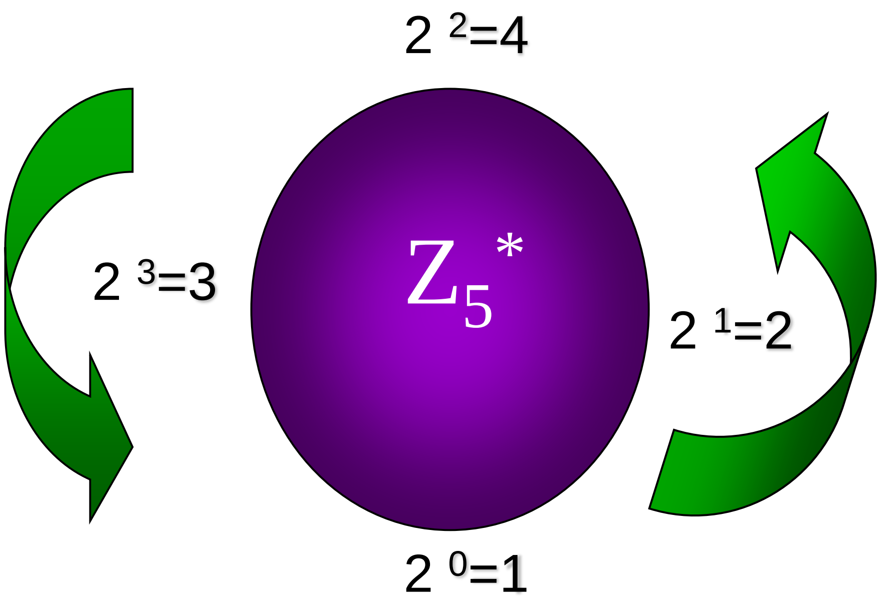
2. If <G> has <u>finite</u> order. Which means that for some $a^h = a^k$



Cyclic Groups: An example

$f(x) = 2^x \pmod 5$ and $x \in Z$;

$2^0 = 1 \pmod 5$
$2^1 = 2 \pmod 5$
$2^2 = 4 \pmod 5$
$2^3 = 3 \pmod 5$
$2^4 = 1 \pmod 5$
$2^5 = 2 \pmod 5$
...



Even if $h \neq k$, still $a^h = a^k$
$h = 1$ and $k = 4$, and $a=2$
$2^1 \pmod 5 = 2^5 \pmod 5$

$$Z_5^* = \{1, 2, 3, 4\}$$

Generators: Definition

- Let p be a prime,
- with an integer *g* such that *g*<p;

  then *g* is a *generator* (mod p)
- if for each integer b from 1 to (p-1),

  there exists some integer a where,

$$g^a \equiv b \pmod{p}.$$

Generators: Example

Let p=11, and g=2, so (p-1)=10, then "a" goes from 1 upto 10

Let's try to obtain all numbers from 1 to 10 in the form of $g^a \equiv b \pmod p$ to see if g=2 is indeed a generator.

$$2^1 \equiv 2 \pmod{11}$$
$$2^2 \equiv 4 \pmod{11}$$
$$2^3 \equiv 8 \pmod{11}$$
$$2^4 \equiv 5 \pmod{11}$$
$$2^5 \equiv 10 \pmod{11}$$
$$2^6 \equiv 9 \pmod{11}$$
$$2^7 \equiv 7 \pmod{11}$$
$$2^8 \equiv 3 \pmod{11}$$
$$2^9 \equiv 6 \pmod{11}$$
$$2^{10} \equiv 1 \pmod{11}$$

Sort it out!

1 2 3 4 5 6 7 8 9 10 YES!
2 is a generator for p=11

Generators: How to Find the Generators?

- For p=11, the other generators are 2,6,7 and 8.

But 3 is not since there is no solution to

$3^a \equiv 2 \pmod{11}$

- Usually it is hard to test whether a given number is a generator or not.

- The easy way is to use the factorization of (p-1).

Generators: How to Find the Generators?

- Let q_1, q_2,…,q_n be the prime factors of (p-1),

Step #1

Find $g^{(p-1)/q}$ (mod p) for all values of $q=q_1,q_2,\ldots,q_n$

Step #2

g is a generator if value does not equal to 1 for any values of q. Otherwise it is not.

Generators:Example #2

- Let p=11, prime factors of (p-1)=10 are 2 and 5.

Testing 2 whether it is a generator:	Testing 3 whether it is a generator:
$2^{(11-1)/2} \pmod{11} = 10$	$3^{(11-1)/2} \pmod{11} = 1$
$2^{(11-1)/5} \pmod{11} = 4$	$3^{(11-1)/5} \pmod{11} = 9$
Neither result is 1, so 2 is a generator.	One result is 1, so 3 is NOT a generator.

Finite Fields

Consists of a finite set of elements for the operations of multiplication and addition which satisfy the below rules:

1. Associativity $a+(b+c) = (a+b)+c$

   $a.(b.c) = (a.b).c$
2. Commutativity $a+b = b+a$

   $a.b = b.a$
3. Distributive law $a.(b+c)=(a.b) + (a.c)$
4. Additive Identity
5. Multiplicative Identity
6. Additive Inverse
7. Multiplicative Inverse

For Example; Z/Z_p → The field of integers modulo a prime number p.

Finite Fields

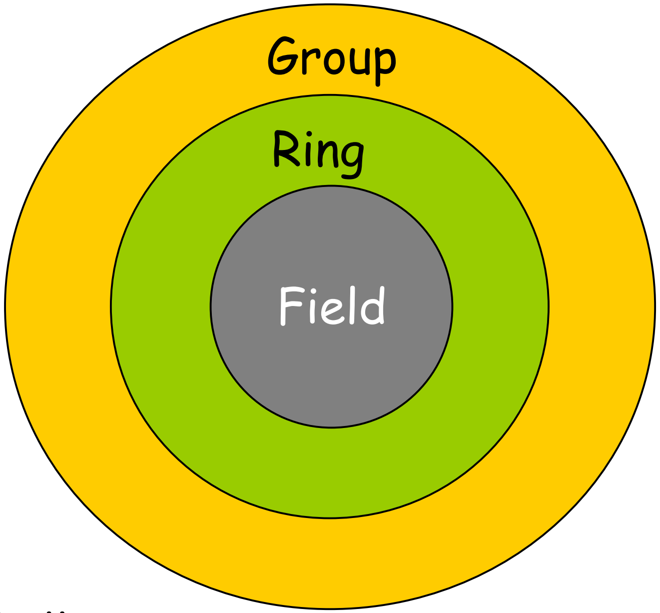
1. The order of finite field is the number of elements in the field.
2. There exists a finite field of order q if and only if q is a prime power. This field is denoted by F_q
3. If $q = p^m$ where p is a prime and m is a positive integer then

   p is called the characteristic of F_q and,

   m is called the extention degree of $F_q = F_{p^m}$

Algebraic Properties

Group - Ring - Field



- Ring;
  - It has created two sets for each + and x operations which are at least two element.
  - Associativity,
  - Distribution .

- Field;
  - It has included all inverse elements of each element in the set for both + and x operation.
  - It is the abelian for + and x operations.

- Group;
  - Closure,
  - Associativity,
  - Identitiy element,
  - Invers element,
  - Abelian (commutative).

Fields

- Let p be a prime number.
- In other case, $p=i.j$ and $1<i \le j < p$ and it is not any x value such that $i.x \equiv 1 \pmod p$. It means that i has not inverse element in Zp set. Hence, Zp is not a field.
- Zp is a cyclic group if and only if p is prime and p>1.

Field

$p=2$

- F_2 , binary fields
- F_{2^m}, extended binary fields
- $Char(F_{2^m})=2$

$p \ge 3$

- F_p prime fields
- F_{p^m} extended prime fields
- $Char(F_{p^m})=p$

  $Char(F_p)=p$

Finite Field Arithmetic

- There are three kinds of fields;
  - Prime Fields
  - Binary Fields
  - Optimal Extention Fields
- There are four basic arithmetic operations;
  - Addition
  - Subtraction
  - Multiplication
  - Inversion

Field Operation

$a,b \in F_q, a-b = a+(-b)$ Where $b+(-b)=0$

and -b is called the **negative** of b.

$a,b \in F, b \neq 0, a/b = a.b^{-1}$ Where $b.b^{-1} = 1$

and b^{-1} is called the **inverse** of b.

Prime Fields

- Let p be a prime number.
- The integers modulo p, consisting of the integers {0,1,2,...,p-1} with addition and multiplication performed modulo p, is a finite order p.
- We denote this field by F_p and call p modulus of F_p.
- For any integers a, a mod p shall denote the unique integer remainder r, $0 \le r \le p-1$, obtained upon dividing a by p; this operation is called **reduction modulo p**.

Example: for the prime field F_{29} ;

Addition: 17+20 = 8 since 37 mod 29 = 8,

Subtraction: 17-20 = 26 since -3 mod 29 = 26,

Multiplication: 17.20 = 21 since 340 mod 29 = 21,

Inversion: 17^{-1}=12 since 17.12 mod 29=1.

Binary Fields

- Finite fields of order 2^m are called **binary fields** or **characteristic-two finite fields**.
- One way to construct F_{2^m} is to use **polynomial basis representation**.
- Binary polynomials whose coefficients are in the field $F_2=\{0,1\}$ of degree at most m-1:

$$F_{2^m} = \{a_{m-1}z^{m-1} + a_{m-2}z^{m-2} + \ldots + a_2z^2 + a_1z^1 + a_0 : a_i \in \{0,1\}\}.$$

Binary Fields

- **Addition** of field elements is the usual addition of polynomials, with coefficient arithmetic modulo 2.

- **Irreducibility;** of $f(z)$ means that $f(z)$ cannot be factored as a product of binary polynomials each of degree less than m.

Binary Fields

- **Reduction polynomial f(z);** it should be **$f(z) = z^m + r(z)$** and f(z) is irreducible.
- **Multiplication** of field elements is performed modulo the **reduction polynomial f(z).** For any binary polynomial a(z), a(z) mod f(z) shall denote unique remainder polynomial r(z) of degree less than m obtained upon long division of a(z) by f(z); this operation is called reduction modulo f(z).

Binary Fields – Plynomial Bases Representation

Addition

$(a_{m-1} \ldots a_1 \ a_0) + (b_{m-1} \ldots b_1 \ b_0) = (c_{m-1} \ldots c_1 \ c_0)$ where each $c_i = a_i + b_i$ over F_2. Addition is just the componentwise XOR of $(a_{m-1} \ldots a_1 \ a_0)$ and $(b_{m-1} \ldots b_1 \ b_0)$.

Subtraction

In the field F_2m, each element $(a_{m-1} \ldots a_1 \ a_0)$ is its own additive inverse, since $(a_{m-1} \ldots a_1 \ a_0) + (a_{m-1} \ldots a_1 \ a_0) = (0 \ldots 0 \ 0)$, the additive identity. Thus addition and subtraction are equivalent operations in F_2m.

Multiplication

$(a_{m-1} \ldots a_1 \ a_0) \ (b_{m-1} \ldots b_1 \ b_0) = (r_{m-1} \ldots r_1 \ r_0)$ where $r_{m-1}x^{m-1} + \ldots + r_1x + r_0$ is the remainder when the polynomial $(a_{m-1}x^{m-1} + \ldots + a_1x + a_0) \ (b_{m-1}x^{m-1} + \ldots + b_1x + b_0)$ is divided by the polynomial $f(x)$ over F_2. (Note that all polynomial coefficients are reduced modulo 2.)

Binary Fields – Plynomial Bases Representation

Exponentiation

The exponentiation $(a_{m-1}\ \ldots\ a_1\ a_0)^e$ is performed by multiplying together ***e*** copies of $(a_{m-1}\ \ldots\ a_1\ a_0)$.

Multiplicative Inversion

There exists at least one element *g* in F_2m such that all non-zero elements in F_2m can be expressed as a power of ***g***. Such an element ***g*** is called a *generator* of F_2m. The multiplicative inverse of an element

$a = g^i$ **is** $a^{-1} = g^{(-i)}$ **mod** $(2^m - 1)$.

Example: Binary Field F_{2^4}

0	z^2	z^3	z^3+z^2
1	z^2+1	z^3+1	z^3+z^2+1
z	z^2+z	z^3+z	z^3+z^2+z
$z+1$	z^2+z+1	z^3+z+1	z^3+z^2+z+1

Addition : $(z^3+z^2+1)+(z^2+z+1)=(z^3+z).$

Subtraction: $(z^3+z^2+1)-(z^2+z+1)=(z^3+z).$

Multiplication:

$$(z^3+z^2+1).(z^2+z+1)=z^5+z+1$$

$$and \quad (z^5+z+1) \ \mathrm{mod}(z^4+z+1) \ = \ z^2+1.$$

Inversion:

$$(z^3+z^2+1)^{-1}=z^2 \Rightarrow$$

$$(z^3+z^2+1).z^2 \ \mathrm{mod}(z^4+z+1)=1.$$

Example: Binary Field F_{2^4}

The elements of F_{2^4} are the 16 vectors:

(0000) (0001) (0010) (0011) (0100) (0101) (0110) (0111) (1000) (1001) (1010) (1011) (1100) (1101) (1110) (1111).

The irreducible polynomial used will be $f(x) = x^4 + x + 1$. The following are sample calculations.

Addition

(0110) + (0101) = (0011).

Multiplication

(1101) (1001)

$= (x^3 + x^2 + 1)(x^3 + 1) \bmod f(x)$

$= x^6 + x^5 + 2x^3 + x^2 + 1 \bmod f(x)$

$= x^6 + x^5 + x^2 + 1 \bmod f(x)$ **(coefficients are reduced modulo 2)**

$= (x^4 + x + 1)(x^2 + x) + (x^3 + x^2 + x + 1) \bmod f(x)$

$= x^3 + x^2 + x + 1$

= (1111).

Example: Binary Field F_{2^4}

Exponentiation

To compute $(0010)^5$, first find

$(0010)^2$
$= (0010)\ (0010)$
$= x\ x \bmod f(x)$
$= (\ x^4 + x + 1)(0) + (x^2) \bmod f(x)$
$= x^2$
$= (0100).$

Then

$(0010)^4$
$= (0010)^2\ (0010)^2$
$= (0100)\ (0100)$
$= x^2\ x^2 \bmod f(x)$
$= (\ x^4 + x + 1)(1) + (x + 1) \bmod f(x)$
$= x + 1$
$= (0011).$

Finally, $(0010)^5$
$= (0010)^4\ (0010)$
$= (0011)\ (0010)$
$= (x + 1)\ (x) \bmod f(x)$
$= (x^2 + x) \bmod f(x)$
$= (\ x^4 + x + 1)(0) + (x^2 + x) \bmod f(x)$
$= x^2 + x$
$= (0110).$

Example: Binary Field F_{2^4}

Multiplicative Inversion

The element g = (0010) is a generator for the field. The powers of g are:

g^0 = (0001) g^1 = (0010) g^2 = (0100) g^3 = (1000) g^4 = (0011)
g^5 = (0110) g^6 = (1100) g^7 = (1011) g^8 = (0101) g^9 = (1010)
g^{10} = (0111) g^{11} = (1110) g^{12} = (1111) g^{13} = (1101)
g^{14} = (1001) g^{15} = (0001).

The multiplicative identity for the field is g^0 = (0001). The multiplicative inverse of :

g^7 = (1011) is $g^{-7 \bmod 15} = g^{8 \bmod 15}$ = (0101).

To verify this, see that

(1011) (0101)
$= (x^3 + x + 1)(x^2 + 1) \bmod f(x)$
$= x^5 + x^2 + x + 1 \bmod f(x)$
$= (x^4 + x + 1)(x) + (1) \bmod f(x)$
$= 1$
= (0001),

which is the multiplicative identity.