Data and Network Security

Course Code: IT-4542

Finite Fields

- It is almost impossible to fully understand practical modern cryptography (AES, RSA, generally public key cryptography) if you do not know what is meant by a finite field.
- And if you do not understand the basics of public-key cryptography, you will not be able to understand
  - the workings of several modern protocols (like the SSH protocol you use everyday for logging into other computers) for secure communications over networks.
  - user and document authentication with certificates.
  - digital rights management
  - Elliptic Curve Cryptography – a replacement for RSA

Finite Fields

- A finite field is a finite set of numbers in which you can carry out the operations of addition, subtraction, multiplication, and division.
- You must know the followings before Finite Fields
  - Set
  - Group, abelian group
  - Ring, commutative ring
  - Integral domain
  - field

Group

A set of objects, along with a binary operation on the elements of the set, must satisfy the following four properties for the set of objects to be called a group:

1. Closure with respect to the operation.

   $a \circ b = c$ is also in the set.

2. Associativity with respect to the operation.

   $$(a \circ b) \circ c = a \circ (b \circ c)$$

3. Identity element

   $$a \circ i = a$$

4. Inverse element

   $$a \circ b = i$$

In general, a group is denoted by $\{G, \circ\}$ where G is the set of objects and $\circ$ the operator.

Examples of infinite groups

- Infinite groups, meaning groups based on sets of infinite size
  - set of all integers
  - for a given value of N, the set of all N × N matrices over real numbers under the operation of matrix addition constitutes a group
  - set of all 3 × 3 nonsingular matrices, along with the matrix multiplication as the operator

Examples of infinite groups

- Let s_n = <1, 2, ..., n> denote a sequence of integers 1 through n.

- Let's now consider the set of all permutations of the sequence s_n. Denote this set by P_n. Each element of the set P_n stands for a permutation <p_1, p_2, p_3, ..., p_{n}> of the sequence s_n.

- Consider, for example, the case when s_3 = <1, 2, 3>. The set of permutations of the sequence s_3 is given by

P_3 = {<1, 2, 3>,<1, 3, 2>,<2, 1, 3>,<2, 3, 1>,<3, 1, 2>,<3, 2, 1>}.

The set P_3 is of size 6. That is the cardinality of P_3 is 6.

- Now let the binary operation on the elements of P_n be that of composition of permutations.

- Let's go back to the example in which the starting sequence is given by $s_3 = <1, 2, 3>$.

- As already shown, each element of P_3 is a distinct permutation of the three integers in s_3. That is,

$$P_3 \quad = \quad \{ \ <p_1, p_2, p_3> \ | \ p_1, p_2, p_3 \in s_3 \ \ with \ \ p_1 \neq p_2 \neq p_3 \ \}$$

- Consider the following two elements π and ρ in the set P_3 of permutations:

$$\begin{aligned} \pi &= < 3, 2, 1 > \\ \rho &= < 1, 3, 2 > \end{aligned}$$

- Let's now consider the following composition of the two permutations π and ρ:

$$\pi \circ \rho \ = \ <3, 2, 1> \ \circ \ <1, 3, 2>$$

$$\pi \circ \rho \;=\; <3,2,1> \circ <1,3,2> \;=\; <2,3,1>$$

Clearly, $\pi \circ \rho \in P_3$.

What About the Other Three Conditions

$$\rho_1 \circ (\rho_2 \circ \rho_3) \;=\; (\rho_1 \circ \rho_2) \circ \rho_3$$

$$<1,2,3> \circ \rho \;=\; \rho \circ <1,2,3> \;=\; \rho$$

$$\rho \circ \pi \;=\; \pi \circ \rho \;=\; \textit{the identity element}$$

ABELIAN GROUPS

$$a \circ b = b \circ a$$

Is the permutation group $\{P_n, \circ\}$ an abelian group? NO

If not for n in general, is $\{P_n, \circ\}$ an abelian group for any particular value of n?

Is the set of all integers, positive, negative, and zero, along with the operation of arithmetic addition an abelian group?

- If the group operation is referred to as addition, then the group also allows for subtraction
- the identity element of such group is frequently denoted by the symbol 0.
- additive inverse of ρ_1 and even denote it by $-\rho_1$

$$\rho_1 + (-\rho_1) = 0$$

RINGS {R,+,×}

- R denotes the set of objects, ’+’ the operator with respect to which R is an abelian group, the ’×’ the additional operator needed for R to form a ring.

- R must be **closed** with respect to the additional operator '$\times$'.

- R must exhibit **associativity** with respect to the additional operator '$\times$'.

- The additional operator (that is, the "multiplication operator") must **distribute** over the group addition operator. That is

$$
\begin{aligned}
a \times (b + c) &= a \times b + a \times c \\
(a + b) \times c &= a \times c + b \times c
\end{aligned}
$$

- The "multiplication" operation is frequently shown by just concatenation in such equations:

$$
\begin{aligned}
a(b + c) &= ab + ac \\
(a + b)c &= ac + bc
\end{aligned}
$$

Examples of Rings

- For a given value of N, the set of all N × N square matrices over the real numbers under the operations of matrix addition and matrix multiplication constitutes a ring.

- The set of all even integers, positive, negative, and zero, under the operations arithmetic addition and multiplication is a ring.

- The set of all integers under the operations of arithmetic addition and multiplication is a ring.

- The set of all real numbers under the operations of arithmetic addition and multiplication is a ring.

Commutative Rings

- A ring is commutative if the multiplication operation is commutative for all elements in the ring. That is, if all a and b in R satisfy the property

$$ab = ba$$

Examples of a commutative ring

- The set of all even integers, positive, negative, and zero, under the operations arithmetic addition and multiplication.

- The set of all integers under the operations of arithmetic addition and multiplication.

- The set of all real numbers under the operations of arithmetic addition and multiplication.

INTEGRAL DOMAIN

An **integral domain** $\{R, +, \times\}$ is a **commutative ring** that obeys the following two additional properties:

- **ADDITIONAL PROPERTY 1:** The set R must include an **identity element** for the **multiplicative operation**. That is, it should be possible to symbolically designate an element of the set R as '1' so that for every element a of the set we can say

$$a1 \;=\; 1a \;=\; a$$

- **ADDITIONAL PROPERTY 2:** Let 0 denote the identity element for the **addition operation**. If a multiplication of any two elements a and b of R results in 0, that is if

$$ab \;=\; 0$$

then either a or b **must be** 0.

Examples of an integral domain

- The set of all integers under the operations of arithmetic addition and multiplication.

- The set of all real numbers under the operations of arithmetic addition and multiplication.

FIELDS

A **field**, denoted $\{F, +, \times\}$, is an **integral domain** whose elements satisfy the following additional property:

- For **every element** a in F, except the element designated 0 (which is the identity element for the '+' operator), there must also exist in F its **multiplicative inverse**. That is, if $a \in F$ and $a \neq 0$, then there must exist an element $b \in F$ such that

$$ab \;=\; ba \;=\; 1$$

Examples of Fields

- The set of all real numbers under the operations of arithmetic addition and multiplication is a field.

- The set of all rational numbers under the operations of arithmetic addition and multiplication is a field.

- The set of all complex numbers under the operations of complex arithmetic addition and multiplication is a field.

- The set of all even integers, positive, negative, and zero, under the operations arithmetic addition and multiplication is NOT a field.

- The set of all integers under the operations of arithmetic addition and multiplication is NOT a field.

Modular Arithmetic

- Given any integer a and a positive integer n, and given a division of a by n that leaves the remainder between 0 and $n - 1$, both inclusive, we define

$$\text{remainder} = a \bmod n$$

- The remainder must be between 0 and $n - 1$, both ends inclusive
- We will call two integers a and b to be congruent modulo n if

$$a \bmod n = b \bmod n$$

$$a \equiv b \pmod{n} \quad \text{//a is congruent to b mod n}$$

$$a \equiv k.n + b \pmod{n}$$

- When a is a divisor of b, we express this fact by $a \mid b$.

Examples of Modular Arithmetic

$$7 \equiv 1 \pmod{3}$$
$$-8 \equiv 1 \pmod{3}$$
$$-2 \equiv 1 \pmod{3}$$
$$7 \equiv -8 \pmod{3}$$
$$-2 \equiv 7 \pmod{3}$$

- The modulo n arithmetic maps all integers into the set $\{0, 1, 2, 3, ..., n-1\}$.

...	0	1	2	0	1	2	0	1	2	0	1	2	0	1	2	0	1	2	0	1	2	0	...
...−	9	−8	−7	−6	−5	−4	−3	−2	−1	0	1	2	3	4	5	6	7	8	9	10	11	12	...

Modular Arithmetic Operations

- The modulo n arithmetic maps all integers into the set $\{0, 1, 2, 3, ..., n - 1\}$

$$[(a \ mod \ n) + (b \ mod \ n)] \ mod \ n = (a + b) \ mod \ n$$
$$[(a \ mod \ n) - (b \ mod \ n)] \ mod \ n = (a - b) \ mod \ n$$
$$[(a \ mod \ n) \times (b \ mod \ n)] \ mod \ n = (a \times b) \ mod \ n$$

Take $a = mn + r_a$, and $b = pn + r_b$

where r_a and r_b are the residues (the same thing as remainders) for a and b, respectively.

Substitute for a and b on the RHS and show how to derive the LHS.

Set of Residues

$$Z_n = \{0, 1, 2, 3, \ldots\ldots, n - 1\}$$

- Memaids
  - The numbers n, $2n$, $3n$, $-n$, $-2n$, etc., are exactly the same number as 0.
  - The number -1 in *mod n* arithmetic, you should think $n - 1$. That is, the number $n - 1$ is exactly the same thing as the number -1 in *mod n* arithmetic.

The Set $Z_n = \{0, 1, 2, 3, ..., n - 1\}$ and its Properties

- Consider the set Z_n along with the following two binary operators defined for the set
  - modulo *n* addition
  - modulo *n* multiplication

- Commutativity:

$$(w + x) \ mod \ n = (x + w) \ mod \ n$$
$$(w \times x) \ mod \ n = (x \times w) \ mod \ n$$

- Associativity:

$$[(w + x) + y] \ mod \ n = [w + (x + y)] \ mod \ n$$
$$[(w \times x) \times y] \ mod \ n = [w \times (x \times y)] \ mod \ n$$

- Distributivity of Multiplication over Addition:

$$[w \times (x + y)] \ mod \ n = [(w \times x) + (w \times y)] \ mod \ n$$

The Set $Z_n = \{0, 1, 2, 3, ..., n-1\}$ and its Properties

- Existence of Identity Elements:

$$(0 + w) \; mod \; n = (w + 0) \; mod \; n = w \; mod \; n$$

$$(1 \times w) \; mod \; n = (w \times 1) \; mod \; n = w \; mod \; n$$

- Existence of Additive Inverses:

For each $w \in Z_n$, there exists a $z \in Z_n$ such that

$$w + z = 0 \; mod \; n$$

What is Z_n?

- Is Z_n a group? If so, what is the group operator?
- Is Z_n an abelian group?
- Is Z_n a ring?
- Actually, Z_n is a commutative ring. Why?
- Why is Z_n not an integral domain?
- Why is Z_n not a field?

Inverses in Z_n

- For every element of Z_n,
  - there exists an additive inverse in Z_n
  - there does not exist a multiplicative inverse for every non-zero element of Z_n.

Z_8	0	1	2	3	4	5	6	7
Additive inverse	0	7	6	5	4	3	2	1
Multiplicative inverse	-	1	-	3	-	5	-	7

- Note: the multiplicative inverses exist for only those elements of Z_n that are relatively prime to n [$gcd(a, n) = 1$].

Some Properties

- modulo *n* addition

  $(a + b) \equiv (a + c)\ (mod\ n)$ implies $b \equiv c\ (mod\ n)$

  – modulo *n* addition always holds, so additive inverses $(-a)$ always exist

- modulo *n* multiplication (NOT obeyed always)

  $(a \times b) \equiv (a \times c)\ (mod\ n)$ does not imply $b \equiv c\ (mod\ n)$

  unless *a* and *n* are relatively prime to each other

  – modulo *n* multiplication conditionally holds, so multiplicative inverses (a^{-1}) conditionally ($gcd(a, n) = 1$) exists.

Euclid's Method for Finding the GCD

- $gcd(\ a,\ a) \ = \ a$

- $if\ \ b|a\ \ then\ \ gcd(\ a,\ b) \ = \ b$

- $gcd(\ a,\ 0) \ = \ a \quad since\ it\ is\ always\ true\ that\ \ a|0$

$$gcd(\ a,\ b) \ = \ gcd(\ b,\ a \bmod b\ )$$

```
gcd( 70, 38 )
    =    gcd( 38, 32 )
    =    gcd( 32, 6 )
    =    gcd( 6, 2 )
    =    gcd( 2, 0 )

Therefore,  gcd( 70, 38 )  = 2
```

```
gcd( 8, 17 ):
    =   gcd( 17, 8 )
    =   gcd( 8, 1 )
    =   gcd( 1, 0 )

Therefore,  gcd( 8, 17 )  = 1
```

Euclid's Method for Finding the GCD

```
gcd( 40902, 24140 )
    =   gcd( 24140, 16762 )
    =   gcd( 16762, 7378 )
    =   gcd( 7378, 2006 )
    =   gcd( 2006, 1360 )
    =   gcd( 1360, 646 )
    =   gcd( 646, 68 )
    =   gcd( 68, 34 )
    =   gcd( 34, 0 )

Therefore,  gcd( 40902, 24140 )  = 34
```

Stein's GCD Algorithm (Binary GCD algorithm)

- If both the integers *a* and *b* are even,

$$gcd(a, b) = 2 \times gcd(a/2, b/2)$$

- If *a* is even and *b* is odd,

$$gcd(a, b) = gcd\ (a/2, b)$$

- If *a* is odd and *b* is even,

$$gcd(a, b) = gcd\ (a, b/2)$$

- If both *a* and *b* are odd and,
  - with $a > b$,

$$gcd(a, b) = gcd\ (a - b, b) = gcd\ ((a - b)/2, b)$$

  - with $a < b$,

$$gcd(a, b) = gcd\ (b - a, a) = gcd\ ((b - a)/2, a)$$

Prime Finite Fields

- Z_n is, in general, a commutative ring.
- Z_n is not a finite field because not every element in Z_n is guaranteed to have a multiplicative inverse.
- An element a of Z_n does not have a multiplicative inverse if a is not relatively prime to the modulus n.
- What if we choose the modulus n to be a prime number?
- Therefore, Z_p is a finite field if we assume p denotes a prime number. Z_p is sometimes referred to as a prime finite field. Such a field is also denoted GF(p), where GF stands for "Galois Field".

Prime Finite Fields

- Z_n has multiplicative identity but it is not be an integral domain

  [$a \times b \equiv 0$ (*mod n*) even when both *a* and *b* are non-zeros]

  [*a* or *b* share common factors with *n*]

- Z_p has multiplicative identity and it is an integral domain

  [$a \times b \equiv 0$ (*mod p*) either *a* or *b* must be zero]

  [*a* or *b* don't have any common factor with *p*]

Multiplicative Inverses for the Elements of Z_p

- If a, $b \in Z_n$,and $a \times b \equiv 1$ (mod n), then both a and b are inverse of each other.
- When n equals a prime p, $gcd(a, n) = 1$ is guaranteed.

- Bezout's Identity

$$gcd\ (a, b) = ax + by$$

Ex: gcd(16, 6) = 2

$$= (-1)\times 16 + 3\times 6$$

a =16, b = 6

x = -1 , y = 3

Multiplicative Inverses for the Elements of Z_p

- If $a, x \in Z_n$,and $a \times x \equiv 1$ ($mod\ n$), then both a (known) and x (to find) are inverse of each other.
- Such that $gcd(a, n) = 1$
- Bezout's Identity

$$ax + ny \ \ \text{mod n} = 1 \text{ mod n}$$

Ex: gcd(16, 6) = 2

$$= (-1)\times 16 + 3\times 6 = 2\times 16 + (-5)\times 6$$

a =16, b = 6

x = -1 , y = 3

gcd(1547, 560).

$$1547 = 2\times 560 + 427$$
$$560 = 1\times 427 + 133$$
$$427 = 3\times 133 + 28$$
$$133 = 4\times 28 + 21$$
$$28 = 1\times 21 + 7$$
$$21 = 3\times 7 + 0$$
↳ Stop.

560) 1547 (2
1120
427) 560 (1
427
133) 427 (3
399
28) 133 (4
112
21) 28 (1
21
7) 21 (3
21
×

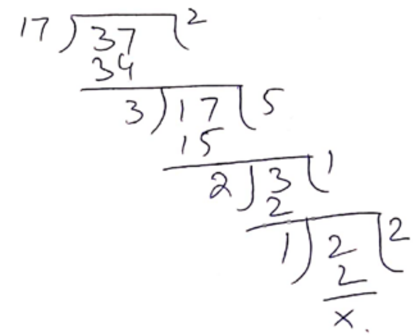
How to write it as a linear combination?

(Move bottom to top)

$$7 = 28 - 1\times 21$$
$$21 = 133 - 4\times 28$$
$$28 = 427 - 3\times 133$$
$$133 = 560 - 1\times 427$$
$$427 = 1547 - 2\times 560$$

$$\begin{aligned}
7 &= 28 - 1\times 21 \\
&= 28 - (133 - 4\times 28) \\
&= 5\times 28 - 1\times 133 \\
&= 5(427 - 3\times 133) - 1\times 133 \\
&= 5\times 427 - 16\times 133 \\
&= 5\times 427 - 16(560 - 1\times 427) \\
&= 21\times 427 - 16\times 560 \\
&= 21(1547 - 2\times 560) - 16\times 560 \\
&= 21\times 1547 - 58\times 560
\end{aligned}$$

$\gcd(37, 17) = 1$



$37 = 2 \times 17 + 3$

$17 = 5 \times 3 + 2$

$3 = 1 \times 2 + 1$

$1 = 3 - 1 \times 2$	$1 = 3 - 1 \times 2$
$2 = 17 - 5 \times 3$	$= 3 - (17 - 5 \times 3)$
$3 = 37 - 2 \times 17$	$= 6 \times 3 - 1 \times 17$
	$= 6(37 - 2 \times 17) - 1 \times 17$
	$= 6 \times 37 - 13 \times 17$

Inverses:

Ex: ~~$17x \equiv 1 \mod 37$~~

$37x \equiv 1 \mod 17$

$x = ?$

$\gcd(37, 17) = 1$

$6 \times 37 - 13 \times 17 \equiv 1 \mod 17$

$6 \times 37 \equiv 1 \mod 17$

$37^{-1} = 6$