Basic Concepts in Number Theory and Finite Fields

Raj Jain
Washington University in Saint Louis
Saint Louis, MO 63130
Jain@cse.wustl.edu

Audio/Video recordings of this lecture are available at:

http://www.cse.wustl.edu/~jain/cse571-11/

1. The Euclidean Algorithm for GCD
2. Modular Arithmetic
3. Groups, Rings, and Fields
4. Galois Fields GF(p)
5. Polynomial Arithmetic

These slides are partly based on Lawrie Brown's slides supplied with William Stalling's book "Cryptography and Network Security: Principles and Practice," 5th Ed, 2011.

Euclid's Algorithm

- Goal: To find greatest common divisor

Example: gcd(10,25)=5 using long division

```
10) 25 (2
    20
    --
  5)10 (2
    10
     --
    00
```

Test: What is GCD of 12 and 105?

Euclid's Algorithm: Tabular Method

		10	25
q_i	r_i	u_i	v_i
0	25	0	1
0	10	1	0
2	5	-2	1
2	0	5	-2

1. Write the first 2 rows. Set $i = 2$.
2. Divide r_{i-1} by r_i, write quotient q_{i+1} on the next row
3. Fill out the remaining entries in the new bottom row:
   a. Multiply r_i by q_{i+1} and subtract from r_{i-1}
   b. Multiply u_i by q_{i+1} and subtract from u_{i-1}
   c. Multiply v_i by q_{i+1} and subtract from previous v_{i-1}

- $r_i = u_i x + v_i y$
- $u_i = u_{i-2} - q_i u_{i-1}$
- $v_i = v_{i-2} - q_i v_{i-1}$
- Finally, If $r_i = 0$, $\gcd(x,y) = r_{i-1}$
- If $\gcd(x, y) = 1$, $u_i x + v_i y = 1 \Rightarrow x^{-1} \bmod y = u_i$
  $\Rightarrow u_i$ is the inverse of x in "**mod *y***" arithmetic.

Euclid's Algorithm Tabular Method (Cont)

- Example 2: Fill in the blanks

		12	105
q_i	r_i	u_i	v_i
0	15	0	1
0	8	1	0
-	-	-	-
-	-	-	-
-	-	-	-

Homework 4A

- **4.19a** Find the multiplicative inverse of 5678 mod 8765

Modular Arithmetic

- $xy \bmod m = (x \bmod m)\,(y \bmod m) \bmod m$
- $(x+y) \bmod m = ((x \bmod m) + (y \bmod m)) \bmod m$
- $(x-y) \bmod m = ((x \bmod m) - (y \bmod m)) \bmod m$
- $x^4 \bmod m = (x^2 \bmod m)(x^2 \bmod m) \bmod m$
- $x^{ij} \bmod m = (x^i \bmod m)^j \bmod m$
- 125 mod 187 = 125
- (225+285) mod 187 = (225 mod 187) + (285 mod 187) = 38+98 = 136
- 125^2 mod 187 = 15625 mod 187 = 104
- 125^4 mod 187 = $(125^2 \bmod 187)^2$ mod 187 = 104^2 mod 187 = 10816 mod 187 = 157
- 128^6 mod 187 = 125^{4+2} mod 187 = (157×104) mod 187 = 59

Modular Arithmetic Operations

- Z = Set of all integers = {…, -2, -1, 0, 1, 2, …}
- Z_n = Set of all non-negative integers less than n = {0, 1, 2, …, n-1}
- Z_2 = {0, 1}
- Z_8 = { 0, 1, 2, 3, 4, 5, 6, 7}
- Addition, Subtraction, Multiplication, and division can all be defined in Z_n
- For Example:
  - (5+7) mod 8 = 4
  - (4-5) mod 8 = 7
  - (5×7) mod 8 = 3
  - (3/7) mod 8 = 5
  - (5*5) mod 8 = 1

Modular Arithmetic Properties

Property	Expression
Commutative laws	$(w + x) \bmod n = (x + w) \bmod n$ $(w \times x) \bmod n = (x \times w) \bmod n$
Associative laws	$[(w + x) + y] \bmod n = [w + (x + y)] \bmod n$ $[(w \times x) \times y] \bmod n = [w \times (x \times y)] \bmod n$
Distributive law	$[w \times (x + y)] \bmod n = [(w \times x) + (w \times y)] \bmod n$
Identities	$(0 + w) \bmod n = w \bmod n$ $(1 \times w) \bmod n = w \bmod n$
Additive inverse $(-w)$	For each $w \in Z_n$, there exists a z such that $w + z = 0 \bmod n$

Homework 4B

- Determine 128^{107} mod 187

Group

- **Group**: A set of elements that is closed with respect to some operation.
- Closed ⇒ The result of the operation is also in the set
- The operation obeys:
  - Obeys associative law: `(a.b).c = a.(b.c)`
  - Has identity `e`: `e.a = a.e = a`
  - Has inverses a^{-1}: $a.a^{-1} = e$
- **Abelian Group**: The operation is commutative

  `a.b = b.a`
- Example: Z_8, + modular addition, identity =0

Cyclic Group

- **Exponentiation**: Repeated application of operator
  - example: $a^3 = a.a.a$
- **Cyclic Group**: Every element is a power of some fixed element, i.e.,

  $b = a^k$ for some a and every b in group

  a is said to be a generator of the group
- Example: {1, 2, 4, 8} with **mod 12** multiplication, the generator is 2.
- $2^0=1$, $2^1=2$, $2^2=4$, $2^3=8$, $2^4=4$, $2^5=8$

Ring

- **Ring**:
  1. A group with two operations: addition and multiplication
  2. The group is abelian with respect to addition: a+b=b+a
  3. Multiplication and additions are both associative:

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

     $$a.(b.c)=(a.b).c$$

  1. Multiplication distributes over addition

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

- **Commutative Ring**: Multiplication is commutative, i.e.,

  $$a.b = b.a$$

- **Integral Domain**: Multiplication operation has an identity and no zero divisors

Ref: http://en.wikipedia.org/wiki/Ring_%28mathematics%29

Homework 4C

- **4.3** Consider the set S = {a, b, c} with addition and multiplication defined by the following tables:

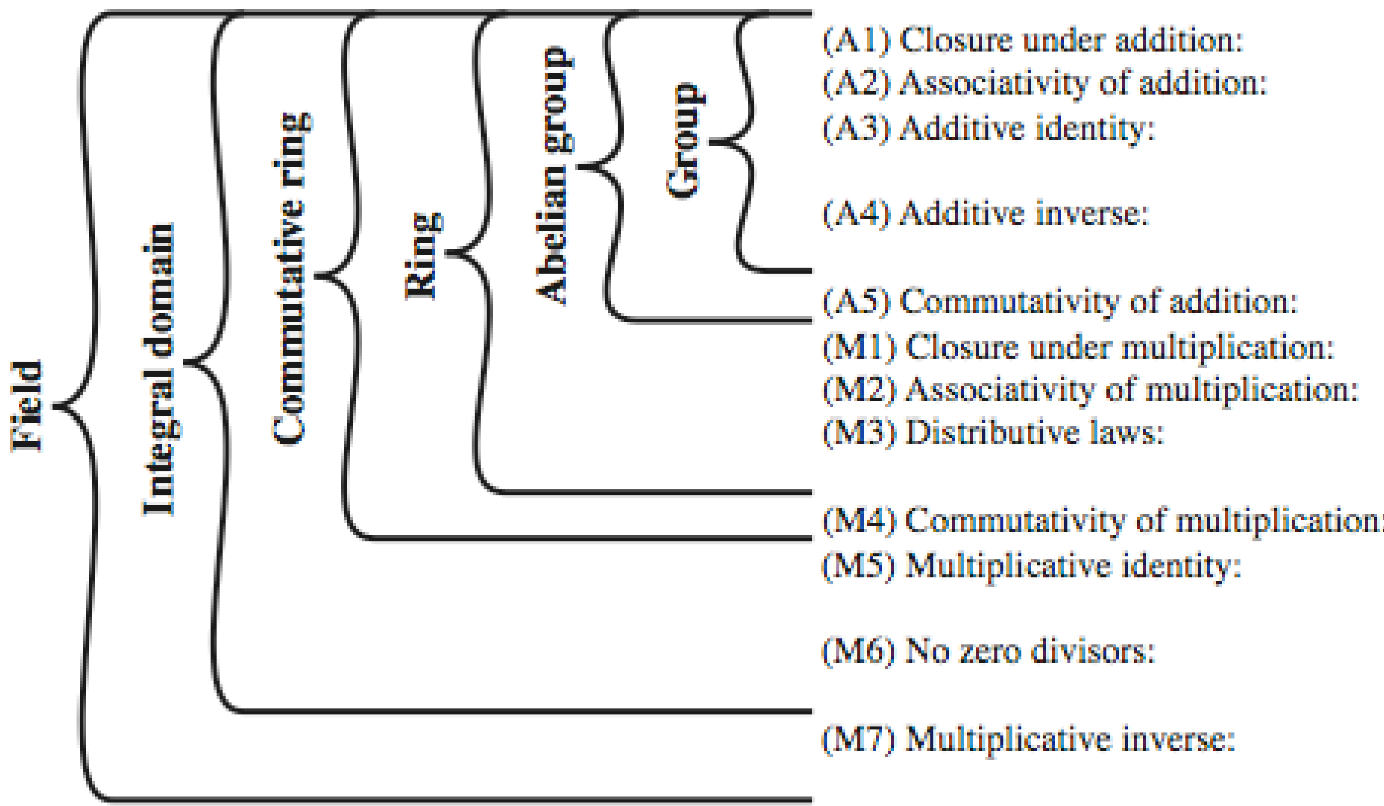
$+$	a	b	c
a	a	b	c
b	b	a	c
c	c	c	a

$\times$	a	b	c
a	a	b	c
b	b	b	b
c	c	b	c

- Is S a ring? Justify your answer.

Field

- **Field**: An integral domain in which each element has a multiplicative inverse.



Finite Fields or Galois Fields

- Finite Field: A field with finite number of elements
- Also known as Galois Field
- The number of elements is always a power of a prime number. Hence, denoted as $GF(p^n)$
- GF(p) is the set of integers {0,1, … , p-1} with arithmetic operations modulo prime p
- Can do addition, subtraction, multiplication, and division without leaving the field GF(p)
- GF(2) = Mod 2 arithmetic
  GF(8) = Mod 8 arithmetic
- There is no GF(6) since 6 is not a power of a prime.

GF(7) Multiplication Example

×	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

Polynomial Arithmetic

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0 = \sum a_i x^i$$

1. Ordinary polynomial arithmetic:
   - Add, subtract, multiply, divide polynomials,
   - Find remainders, quotient.
   - Some polynomials have no factors and are prime.
2. Polynomial arithmetic with **mod p** coefficients
3. Polynomial arithmetic with **mod p** coefficients and mod m(x) operations

Polynomial Arithmetic with Mod 2 Coefficients

- All coefficients are 0 or 1, e.g.,

  let $f(x) = x^3 + x^2$ and $g(x) = x^2 + x + 1$

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

  $f(x) \times g(x) = x^5 + x^2$
- **Polynomial Division**: $f(x) = q(x)\, g(x) + r(x)$
  - can interpret $r(x)$ as being a remainder
  - $r(x) = f(x) \bmod g(x)$
  - if no remainder, say $g(x)$ divides $f(x)$
  - if $g(x)$ has no divisors other than itself & 1 say it is **irreducible** (or prime) polynomial
- Arithmetic modulo an irreducible polynomial forms a finite field
- Can use Euclid's algorithm to find gcd and inverses.

Example GF(2^3)

Table 4.7 Polynomial Arithmetic Modulo ($x^3 + x + 1$)

(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	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

(b) Multiplication

		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	$x+1$

Computational Example in $GF(2^n)$

- Since coefficients are 0 or 1, any polynomial can be represented as a bit string
- In $GF(2^3)$, (x^2+1) is 101_2 & (x^2+x+1) is 111_2
- Addition:
  - $(x^2+1) + (x^2+x+1) = x$
  - 101 XOR 111 = 010_2
- Multiplication:
  - $(x+1).(x^2+1) = x.(x^2+1) + 1.(x^2+1)$
    $= x^3+x+x^2+1 = x^3+x^2+x+1$
  - 011.101 = (101)<<1 XOR (101)<<0 =
    1010 XOR 101 = 1111_2
- Polynomial modulo reduction (get q(x) & r(x)) is
  - (x^3+x^2+x+1) mod $(x^3+x+1) = 1.(x^3+x+1) + (x^2) = x^2$
  - 1111 mod 1011 = 1111 XOR 1011 = 0100_2

Homework 4D

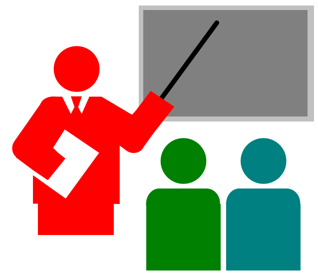
- **4.25d** Determine the gcd of the following pairs of polynomials over GF(11)

$$5x^3+2x^2-5x-2 \text{ and } 5x^5+2x^4+6x^2+9x$$

Using a Generator

- A **generator** g is an element whose powers generate all non-zero elements
  - in F have 0, g^0, g^1, …, g^{q-2}
- Can create generator from **root** of the irreducible polynomial then adding exponents of generator

Summary



1. Euclid's tabular method allows finding gcd and inverses
2. Group is a set of element and an operation that satisfies closure, associativity, identity, and inverses
3. Abelian group: Operation is commutative
4. Rings have two operations: addition and multiplication
5. Fields: Commutative rings that have multiplicative identity and inverses
6. Finite Fields or Galois Fields have p^n elements where p is prime
7. Polynomials with coefficients in GF(2n) also form a field.