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/cse571-17/

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," 7th Ed, 2017.

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

		x	y
		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 $r_i = 0$, $\gcd(x,y) = r_{i-1}$

Euclid's Algorithm Tabular Method (Cont)

- Example 2: Fill in the blanks

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

Tabular Method (Cont)

- Example 2: Fill in the blanks

		8	15
q_i	r_i	u_i	v_i
	15	0	1
	8	1	0
1	7	-1	1
1	1	2	-1
7	0	-15	-8

- GCD(8,15) = 1
- $r_i = u_i x + v_i y$
- If gcd(x, y) = 1, 1=2*8-1*15 or 2*8 = 1+1*15
- 2*8 mod 15 = (1+1*15)mod 15 = 1 ⇒ Inverse of 8 = 2 mod 15
- In general, $u_i x + v_i y = 1 \Rightarrow x^{-1} \bmod y = u_i$
  ⇒ u_i is the inverse of x in "**mod *y***" arithmetic.

Homework 4A

- Find the multiplicative inverse of 5678 mod 8765
- Do it on your own. Do not submit.
- Answer: 2527

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
- 125^6 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 125^{107} mod 187
- Do it on your own. Do not submit.
- Answer: 5

Group

- **Group**: A set of elements that is closed with respect to some operation.
- Closed $\Rightarrow$ 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

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

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

- **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

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

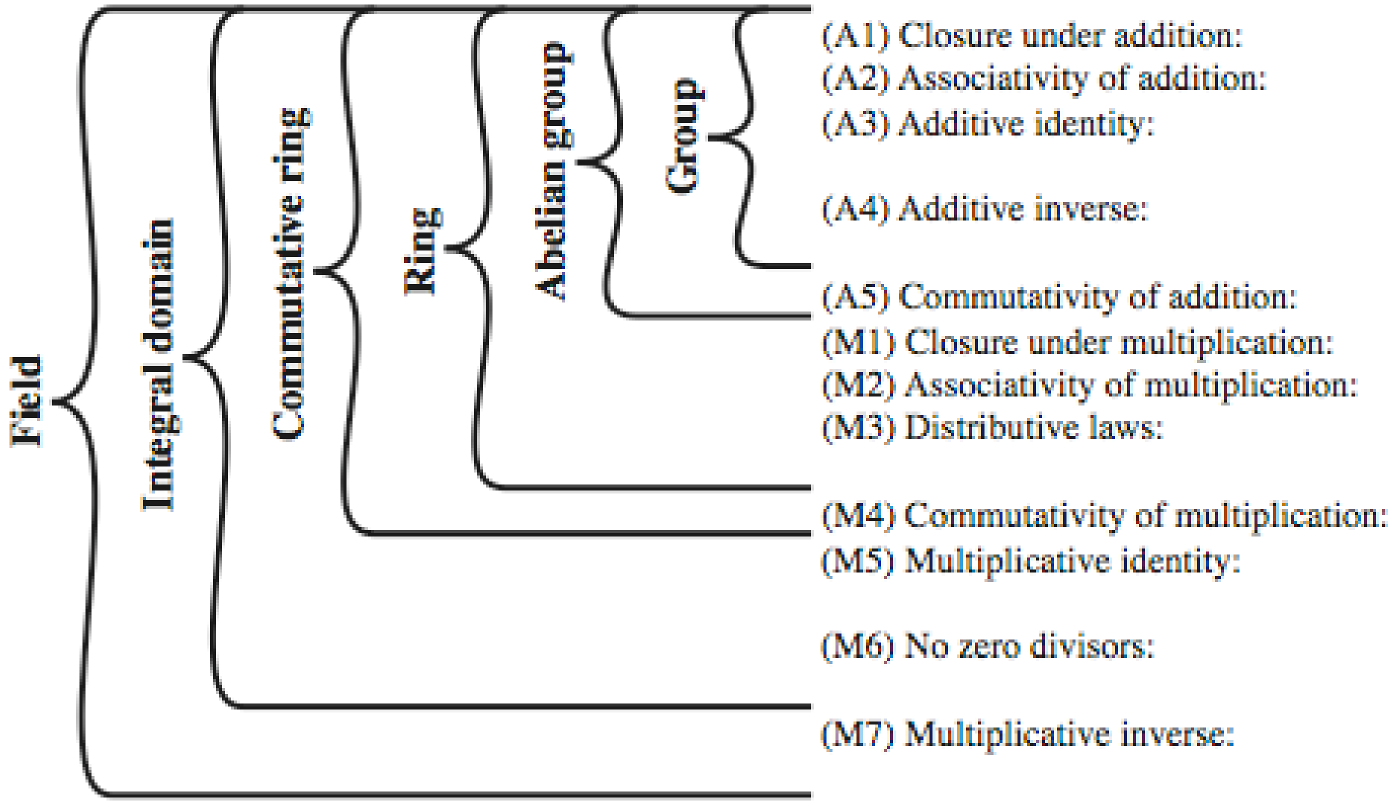
$+$	a	b	c
a	a	b	c
b	b	a	c
c	c	c	a

$\times$	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 $\{0, 1, \ldots, p\text{-}1\}$ 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, where m(x) is a n^{th} degree polynomial = GF(p^n)

Polynomial Arithmetic with Mod 2 Coefficients

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

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

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

  $f(x) \times g(x) = x^5 + x^2$

$$
\begin{array}{r}
(x^2 + x + 1) \times (x^3 + x^2) \\
\hline
x^5 + x^4 + x^3 \qquad \\
+ x^4 + x^3 + x^2 \\
\hline
x^5 + \qquad\qquad + x^2
\end{array}
$$

- **Polynomial Division**: $f(x) = q(x)\, g(x) + r(x)$

$$
\begin{array}{l}
x^3 + x + 1)\, x^4 + x^3 + x + 1\, (x + 1 \\
\qquad\qquad\; x^4 + x^2 + x \\
\hline
\qquad\qquad\; x^3 + x^2 + 1 \\
\qquad\qquad\; x^3 + x + 1 \\
\hline
\qquad\qquad\; x^2 + x
\end{array}
$$

  - $r(x)$ = remainder
    $= f(x) \bmod g(x)$
  - 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(2n)

- 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:
  - $(x^2+1) + (x^2+x+1) = x$
  - $101 \oplus 111 = 010_2$
- Multiplication:
  - $(x+1).(x^2+1) = x.(x^2+1) + 1.(x^2+1)$
    $= x^3+x+x^2+1 = x^3+x^2+x+1$
  - $011.101 = 1111_2$
- Polynomial modulo reduction (get $q(x)$ & $r(x)$) is
  - (x^3+x^2+x+1) mod $(x^3+x+1) = 1.(x^3+x+1) + (x^2) = x^2$
  - $1111 \bmod 1011 = 1111 \oplus 1011 = 0100_2$

Homework 4D

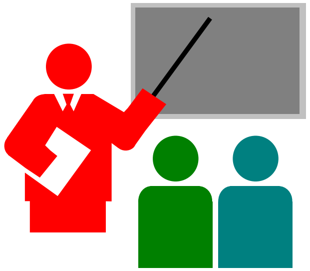
- Determine the gcd of the following pairs of polynomials over GF(11)

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

Using a Generator

- A **generator** g is an element whose powers generate all non-zero elements in F
  $F=\{0, g^0, g^1, \ldots, g^{q-2}\}$
- 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(2^n) also form a field.

Lab 4: Brute Force Password Cracking

Goal: Find user passwords from the password file.

This lab consists of using the following two tools:

1. Password dump Pwdump7 to retrieve the password file, http://www.openwall.com/passwords/microsoft-windows-nt-2000-xp-2003-vista-7#pwdump
2. John the ripper V1.8, Brute force password cracker to decode the entry http://www.openwall.com/john/

Throughout the lab, please note down the commands as indicated so that you can submit them as the solution.

- Remote desktop via VPN to CSE571XPS
- Use the common student account

Step 1: Get the Password File

- Read about pwdump
- Remote access the student account on CSE571XPS, open Command Prompt
- CD to c:/
- Run pwdump7 -h to get some help
- Run pwdump7 with appropriate parameters to get the hash file from CSE571XPS. Note down the command you used.
- Open the hash file obtained in notepad. Delete all lines except the one with your last name.
- Save the file as c:\john180\run\<your_last_name>.txt
- Delete the original full hash file that you downloaded

Step 2: Find Your Password

- CD to c:\john180\run
- Delete john.pot and john.log, if present.
- Run John to get help and read all the options
- Run John with the file you created in step 1
  - Your password is CseXXXX where X is a decimal digit [0-9].
  - Use correct options to search only for the specified pattern. (Otherwise, John will take very long)
  - If John takes more than one minute to finish then you have not chosen the correct options
- After John finishes. Note down the contents of john.pot file and submit. Delete your hash file, john.pot, and john.log

3. Change Your Password

- Logout from the common student account and close your remote desktop connection
- Start a new remote desktop connection using your last name as username and the password you obtained in Step 2.
- **Change your password** to a stronger password of your choice. Do this from your own account (not the common student account).
- Note the time and date you change the password. Submit the time as answer.
- Logout and close your remote desktop connection

Scan This to Download These Slides

Raj Jain

http://rajjain.com

Related Modules

CSE571S: Network Security (Spring 2017),
http://www.cse.wustl.edu/~jain/cse571-17/index.html

CSE473S: Introduction to Computer Networks (Fall 2016),
http://www.cse.wustl.edu/~jain/cse473-16/index.html

Wireless and Mobile Networking (Spring 2016),
http://www.cse.wustl.edu/~jain/cse574-16/index.html

CSE571S: Network Security (Fall 2014),
http://www.cse.wustl.edu/~jain/cse571-14/index.html

Audio/Video Recordings and Podcasts of
Professor Raj Jain's Lectures,
https://www.youtube.com/channel/UCN4-5wzNP9-ruOzQMs-8NUw