W4 Number Theory

September 30, 2020 12:34 PM

Outline

- Concept of groups, rings, and fiels
- Modular arithmetic with integers
- Finite fields GF(p)
- Polynomial arithmetic in general and in GF(2^n)
- Prime number
- Fermat's & Euler's Theorem & phy(n)
- Primitive roots

Introduction

Groups

- ### General
- Define: groups
  A set of elements with a binary operation denoted by • that associates to each ordered pair (a,b) of elements in G an element (a • b) in G, such that the following axioms are obeyed:
  a. A1 - Closure
  $$a, b \in G \rightarrow a \cdot b \in G$$
  b. A2 - Associate
  $$a \cdot (b \cdot c) = (a \cdot b) \cdot c, for\ all\ a, b, c \in G$$
  c. A3 - Identity element
  $$\exists e \in G, st.\ a \cdot e = e \cdot a = a\ for\ \forall a$$
  d. A4 - Inverse element
  $$\forall a, \exists a' st.\ a \cdot a' = a' \cdot a = e$$
  e. A5 - For Abelian group: commutative
  $$a \cdot b = b \cdot a, for\ all\ a, b \in G$$

- ### Cyclic group
- Define: exponentiation a^n
- Identity e = a^0
- Cyclic group:
  - $b = a^k, for\ some\ a\ and\ every\ b \in G$, k is integer
  - a: generator of the group
  - Cyclic ∈ abelian, fini/inf

Rings

- Define: ring R
  - {R, +, x}
  - 2 binary operations
    - Addition
    - Multiplication
  - Obey:

        - A1 - A5: Abelian group
        - M1 - Closure under multiplication

          $a, b \in R \rightarrow ab \in R$

        - M2 - Associativity of multiplication

          $a(bc) = (ab)c, for\ all\ a, b, c \in R$
        - M3 - Distributive laws

          $a(b + c) = ab + ac\ , for\ all\ a, b, c \in R$

          $(a + b)c = ac + bc, for\ all\ a, b, c \in R$
        - Subtraction also applied

          $a - b = a + (-b)$

- Commutative rings
    - Rings
    - M4 - Commutativity of multiplication

      ab = ba, for all a, b $\in R$
- Integral domain
    - Commutative rings
    - M5 - Multiplicative identity

      $\exists 1 \in R, st.\ a1 = 1a = a\ for$ all $a \in R$
    - M6 - No zero divisors

      $a, b \in R\ \&\ ab = 0 \rightarrow a = 0\ or\ b = 0\ or\ a = b = 0$

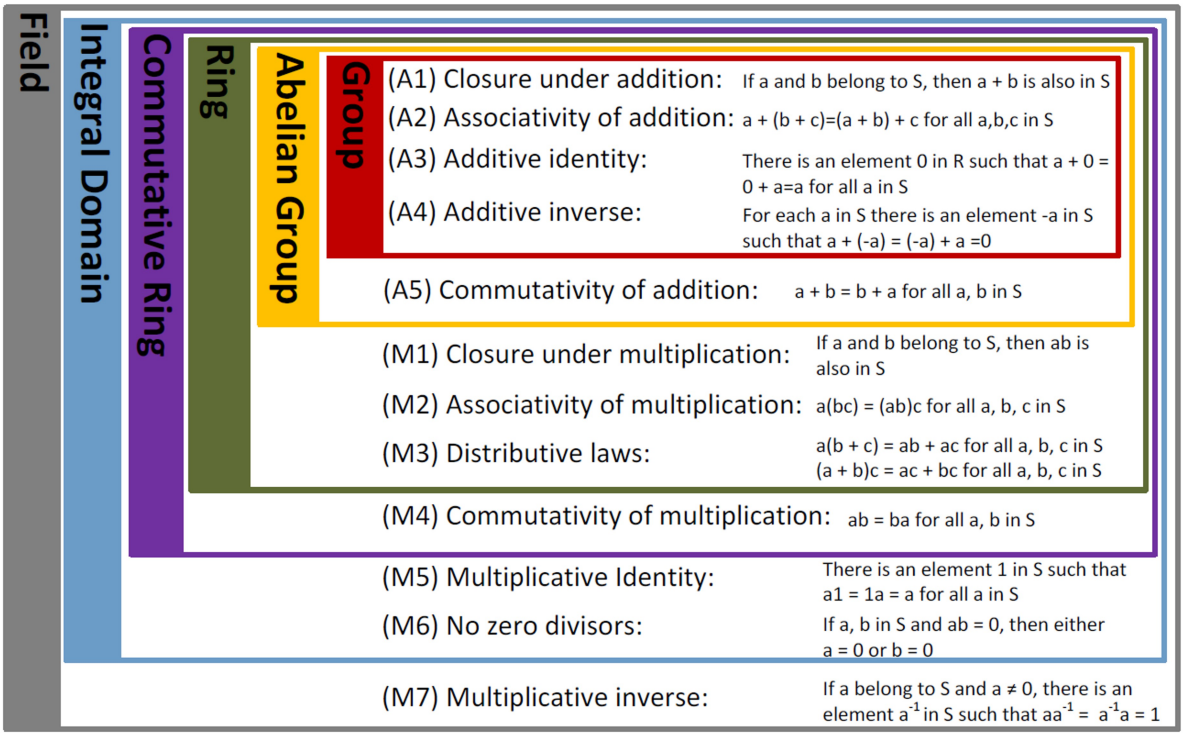
Fields

- Define: field F
    - {F, +,×}
    - 2 binary operations
        - Addition
        - Multiplication
    - A1 - M6
    - M7 - Multiplicative inverse

      $\forall a \in F, except\ 0, \exists a^{-1} \in F, st.\ aa^{-1} = a'a = 1$
    - Division also applied.

      $a/b = ab^{-1}$

Groups, Rings, & Fields



Divisibility and Division Algorithm

- $a = mb \leftrightarrow b|a$: b *divides* a
- b: divisor
- $\frac{a}{n} = qn + r, 0 \leq r < n$

GCD: Greatest Common Divisor

- E.g. GCD(60, 24) = 12
- No common factor --> relatively prime
  - E.G. GCD(8, 15) = 1
- Euclidean Algorithm --> calculate GCD

Modular Arithmetic

Basic

- modulo operator: a mod n --> remainder, n: modulus
- $a \bmod n = b \bmod n \leftrightarrow a = b (\bmod n) \leftrightarrow a, b$ *congruent modulo* n
- a = qn + b, b: residue, usually smallest.
- -12 mod 7 =-5 mod 7 =2 mod 7 =9 mod 7 --> modulo reduction

Modular Arithmetic Operations

- Arithmetic with residue
- Finite
- +, x, modulo reduction
- $(a \pm b) \bmod n = [a \bmod n \pm b \bmod n] \bmod n$
- $(a \times b) \bmod n = [a \bmod n \times b \bmod n] \bmod n$

Modular Arithmetic

- the set of residues: $Z_n = \{0, 1, \ldots, n-1\}$
- commutative ring for addition with a multiplicative identity
- $(a + b) = (a + c) \bmod n \rightarrow b = c \bmod n$
- $(a \times b) = (a \times c) \bmod n \;\&\; (a, n)$ *relatively prime* $\rightarrow b = c \bmod n$

$a = xy$
$n = zy$

$$\frac{xy \cdot b}{zy} = \frac{xb}{z}$$

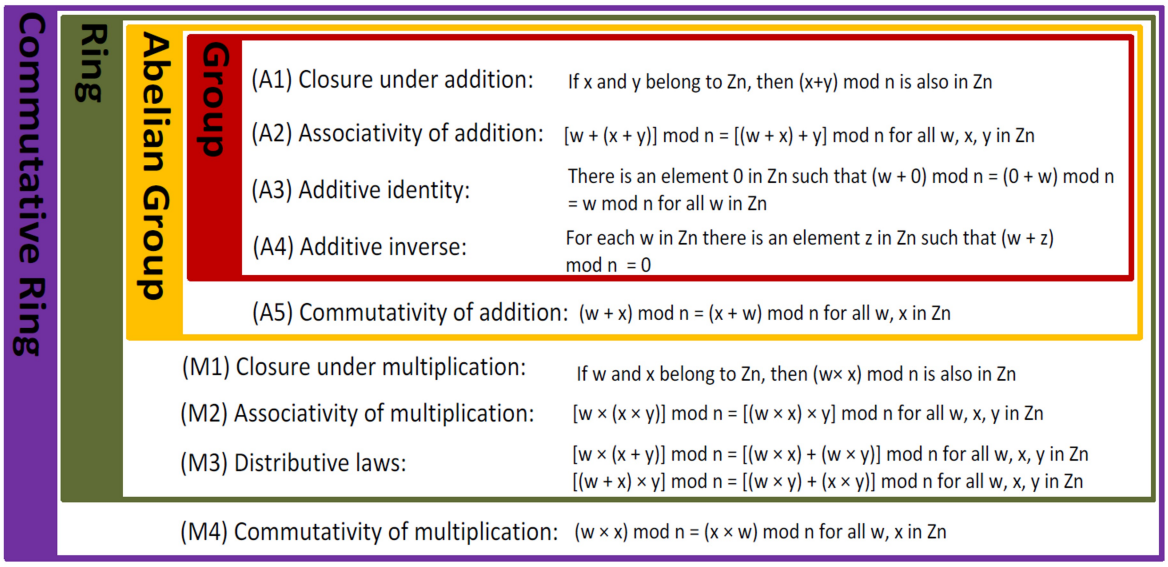
$$\frac{xy \cdot c}{zy} = \frac{xc}{z}$$

$\times x$

$$\Rightarrow (xb) \equiv (x \cdot c) \pmod{z}$$

- 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 $w + z = 0 \bmod n$



- Inverse Example
- Modulo 8 Addition Example

+	0	1	2	3	4	5	6	7
0	0	1	2	3	4	5	6	7
1	1	2	3	4	5	6	7	0
2	2	3	4	5	6	7	0	1
3	3	4	5	6	7	0	1	2

e.g.

$(2+6) \bmod 8 = 0$

+	0	1	2	3	4	5	6	7
0	0	1	2	3	4	5	6	7
1	1	2	3	4	5	6	7	0
2	2	3	4	5	6	7	0	1
3	3	4	5	6	7	0	1	2
4	4	5	6	7	0	1	2	3
5	5	6	7	0	1	2	3	4
6	6	7	0	1	2	3	4	5
7	7	0	1	2	3	4	5	6

e.g.

$(2+6) \bmod 8 = 0$

- Additive inverse: (x + y) mod z = 0

- Modulo 8 Multiplication Example

×	0	1	2	3	4	5	6	7
0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7
2	0	2	4	6	0	2	4	6
3	0	3	6	1	4	7	2	5
4	0	4	0	4	0	4	0	4
5	0	5	2	7	4	1	6	3
6	0	6	4	2	0	6	4	2
7	0	7	6	5	4	3	2	1

e.g.

$(3 \times 3) \bmod 8 = 1$

- Multiplicative Inverse: (x * y) mod z = 1
- Additive and Multiplicative Inverses Modulo 8

w	$-w$	w^{-1}
0	0	—
1	7	1
2	6	—
3	5	3
4	4	—
5	3	5
6	2	—
7	1	7

Galois Fields

- number of elements in a finite field must be a power of a prime, p^n(n is a positive number)
- GF(p^n)
- Often used:
  - GF(p)
  - GF(2^n)

- Galois Fields GF(p)
- {0,1, … , p-1} + mod p
- finite field
  - multiplicative inverses: all integer in Zn relatively prime to p
- addition, subtraction, multiplication, division ❤️
- 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

e.g.

$2^{-1} = 4$ since

$2 \cdot 4 = 8 = 1 \mod 7$

Polynomial Arithmetic

1. Ordinary polynomial arithmetic: basic rules of algebra
2. On mod p: coefficients --> GF(p)
3. Coe: GF(p), && polynomial m(x)

- Ordinary Polynomial Arithmetic

- E.g.
  $f(x) = x^3 + x^2 + 2 \; and \; g(x) = x^2 - x + 1$

  $f(x) + g(x) = x^3 + 2x^2 - x + 3$

  $f(x) \times g(x) = x^5 + 3x^2 - 2x + 2$

Polynomial Arithmetic With Coefficients in Z_p

- On rings
- On fields: division possible
  - Not fields: division not always defined

Polynomial Division

- *Any polynomial:* $f(x) = q(x)g(x) + r(x) \; \leftrightarrow r(x) \; remainder \; \leftrightarrow r(x) = f(x) \; mod \; g(x)$
- No r(x) --> g(x) divides f(x)
  - g(x) | f(x)
  - g(x) is a factor/divisor of f(x)
  - No divisor (except 1 & itself): irreducible(or prime) polynomial
- arithmetic modulo an irreducible polynomial forms a field

Polynomial GCD

- GCD(a(x), b(x)) = c(x) if:
  - c(x) | a(x) && c(x) | b(x)
  - d(x) | a(x) && d(x) | b(x) ---> d(x) | c(x)
- <---> gcd[a(x), b(x)] is the polynomial of maximum degree that divides both a(x)and b(x)
- Euclidean algorithm --> gcd[a(x), b(x)], coe in field

GF(2^n)

- Cryptographic: integers
- GF(2^n): the set of polynomials of degree n-1 with coefficients in Z_2={0,1}, addition and multiplication are defined modulo irreducible m(x) of degree n
- E.g.

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

+	000 0	001 1	010 x	011 $x+1$	100 x^2	101 x^2+1	110 x^2+x	111 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

(a) Addition

×	000 0	001 1	010 x	011 $x+1$	100 x^2	101 x^2+1	110 x^2+x	111 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	$x+1$

(b) Multiplication

e.g. $100 \times 010 = x^2 \cdot x = x^3 \Rightarrow x^3 \bmod (x^3+x+1) = x+1$

- Computational Considerations
- Coefficient: 0, 1 --> bit string
- Add: XOR
- Multiply: shift & XOR
- modulo reduction: substituting highest power with remainder repeatedly
- GF(2^n): $x^n \bmod g(x) = g(x) - x^n$
- Computational Example
- GF(2^3):

$x^2 + 1 = 101_2$
$x + 1 = 011_2$
$m(x) = x^3 + x + 1 = 1011$

Addition:

$(x^2+1) + (x+1) = x^2 + x \leftrightarrow 101\ XOR\ 011 = 110_2$

Multiplication:

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

$\Leftrightarrow 101 \cdot 011 = 101(010 \oplus 001)$

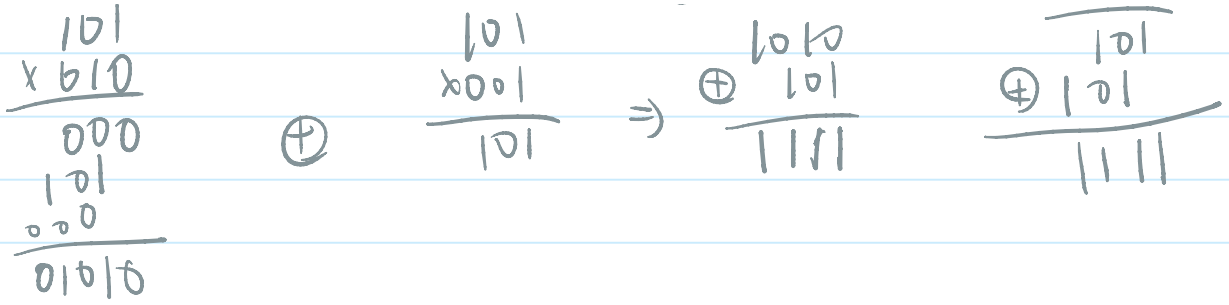
101 × 010

101 × 001

1010 ⊕ 101

OR

101 × 011 = 101 ⊕ 1010 ⊕ 101



polynomial modulo reduction: obtain q(x) & r(x)

$(x^3 + x^2 + x + 1) = 1 \cdot (x^3 + x + 1) + x^2$

$(x^3 + x^2 + x + 1) = x^2 \ mod\ (x^3 + x + 1), q(x) = 1, r(x) = x^2$

Prime Numbers

- Divisors: 1 & itself

```
2  3  5  7  11 13 17 19 23 29 31 37 41 43 47 53
59 61 67 71 73 79 83 89 97 101 103 107 109
113 127 131 137 139 149 151 157 163 167 173
179 181 191 193 197 199
```

- ### Prime Factorization
- Factor: n = a * b * c
- The prime factorisation: product of prime
  E.g. 3600= 9×4×100=3×3×2×2×2×2×5×5 = $=2^4 \times 3^2 \times 5^2$
- ### Relatively Prime Numbers & GCD
- a, b common divisor: only 1 --> relatively prime
- ---> determine GCD
  - E.g.
    $300 = 2^2 \times 3^1 \times 5^2$

    $18 = 2^1 \times 3^2$

    $\gcd(18, 300) = 2^1 * 3^1 * 5^0 = 6$

- ### Fermat's Theorem
- $a^{p-1} \equiv 1\ (mod\ p)$
  - p: prime
  - a: N+
  - Gcd(a, p) = 1
- $alternative\ form:\ a^p \equiv$ a mod p
- --> public key cryptography

- ### Euler's Totient Function φ(n)
- Mod n:
  - Complete set of residue: {0, 1, …, n-1}
  - Reduced set of residue: relatively prime to n
    - E.g. n=10
      - C o s: {0, 1, …, 9}

- R o s: {1, 3, 5, 7, 9}

- # of elements in reduced set of residue = Euler's Totient Function $\varphi(n)$
- Calculate φ(n)

1. P is prime: $\varphi(p) = p - 1$
   E.g. $\varphi(37) = 36$
2. N = p * q, pq prime: $\varphi(pq) = (p-1)(q-1)$
   Eg. $\varphi(21) = (3-1)*(7-1) = 12$
3. General: prime factorization

- ## Euler's Theorem
- Generalisation of Fermat's Theorem
- $a^{\varphi(n)} \equiv 1 \ (mod\ n)$
  - For any a,n if gcd(a,n)=1
  - Eg. a=3, n=10, $\varphi(10) = (2-1)*(5-1) = 4$ → 3^4 = 81 = 1 mod 10
    Eg. a=2, n=11, $\varphi(11) = 10$ --> 2^10 = 1,024 = 1 mod 11

- ## Chinese Remainder Theorem (CRT)
- Eg.
  Z10 = {0, 1, …, 9}
  Can be reconstructed from two residues mod 2 and 5 (relatively prime factors of 10)
  For example, x mod 2 = 0 && x mod 5 = 3 --> x=8 unique

- ## Powers of an Integer, Modulo n
  7=7(mod 19)
  7^2 = 49 = 2*19 + 11 = 11(mod 19)
  7^3 = 343 = 18*19+1 = 1(mod 19)
  7^4 = 2,401 = 7 (mod 19)
  7^5 = 11(mod 19)
  --> 7^m = 1(mod 19) when m = 3i, i=1, 2, …

- ## Primitive Roots
- Euler's theorem: $a^{\varphi(n)} \bmod n = 1$
- Think: a^m = 1 (mod n) && gcd(a, n)
  m = ϕ(n) or maybe smaller --> cycle
- Smallest m = ϕ(n) --> a = primitive root
- if n is prime, then successive powers of a primitive root "generate" all residues mod n

Powers of Integers, Modulo 19

$\phi(19) = 18$

a	a^2	a^3	a^4	a^5	a^6	a^7	a^8	a^9	a^{10}	a^{11}	a^{12}	a^{13}	a^{14}	a^{15}	a^{16}	a^{17}	a^{18}
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
2	4	8	16	13	7	14	9	18	17	15	11	3	6	12	5	10	1
3	9	8	5	15	7	2	6	18	16	10	11	14	4	12	17	13	1
4	16	7	9	17	11	6	5	1	4	16	7	9	17	11	6	5	1
5	6	11	17	9	7	16	4	1	5	6	11	17	9	7	16	4	1
6	17	7	4	5	11	9	16	1	6	17	7	4	5	11	9	16	1
7	11	1	7	11	1	7	11	1	7	11	1	7	11	1	7	11	1
8	7	18	11	12	1	8	7	18	11	12	1	8	7	18	11	12	1
9	5	7	6	16	11	4	17	1	9	5	7	6	16	11	4	17	1
10	5	12	6	3	11	15	17	18	9	14	7	13	16	8	4	2	1
11	7	1	11	7	1	11	7	1	11	7	1	11	7	1	11	7	1
12	11	18	7	8	1	12	11	18	7	8	1	12	11	18	7	8	1
13	17	12	4	14	11	10	16	18	6	2	7	15	5	8	9	3	1
14	6	8	17	10	7	3	4	18	5	13	11	2	9	12	16	15	1
15	16	12	9	2	11	13	5	18	4	3	7	10	17	8	6	14	1
16	9	11	5	4	7	17	6	1	16	9	11	5	4	7	17	6	1
17	4	11	16	6	7	5	9	1	17	4	11	16	6	7	5	9	1

m=9
m=6
m=18
n=18
↳ primitive root

15	16	12	9	2	11	13	5	18	4	3	7	10	17	8	6	14	1
16	9	11	5	4	7	17	6	1	16	9	11	5	4	7	17	6	1
17	4	11	16	6	7	5	9	1	17	4	11	16	6	7	5	9	1
18	1	18	1	18	1	18	1	18	1	18	1	18	1	18	1	18	1

Summary

- Groups, rings, fields
- Mod
- GF(p)
- Poly GF(2^n)
- Prime #
- Fermat / Euler
- Miller-Rabin Algorithm(?) --> tb
- CRT
- Primitive Roots