Number Theory

Group

- A set S of elements or “numbers” may be finite or infinite with binary operation ‘.’ so G=(S,.)
- Obeys CAIN:
  - Closure : a,b in S, then a.b in S
  - Associative law :(a.b).c = a.(b.c)
  - has Identity e :e.a = a.e = a
  - has Inverses a-1 :$a.a^{-1} = e$
- if commutative a.b = b.a
  - then forms an abelian group

Cyclic Group

- A group is cyclic if every element is a power of some fixed element

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

- a is said to be a generator of the group

Ring

- a set of "numbers" with two operations (addition and multiplication) which form:
- an abelian group with addition operation and multiplication:
  - has closure
  - is associative
  - distributive over addition: $a(b+c) = ab + ac$

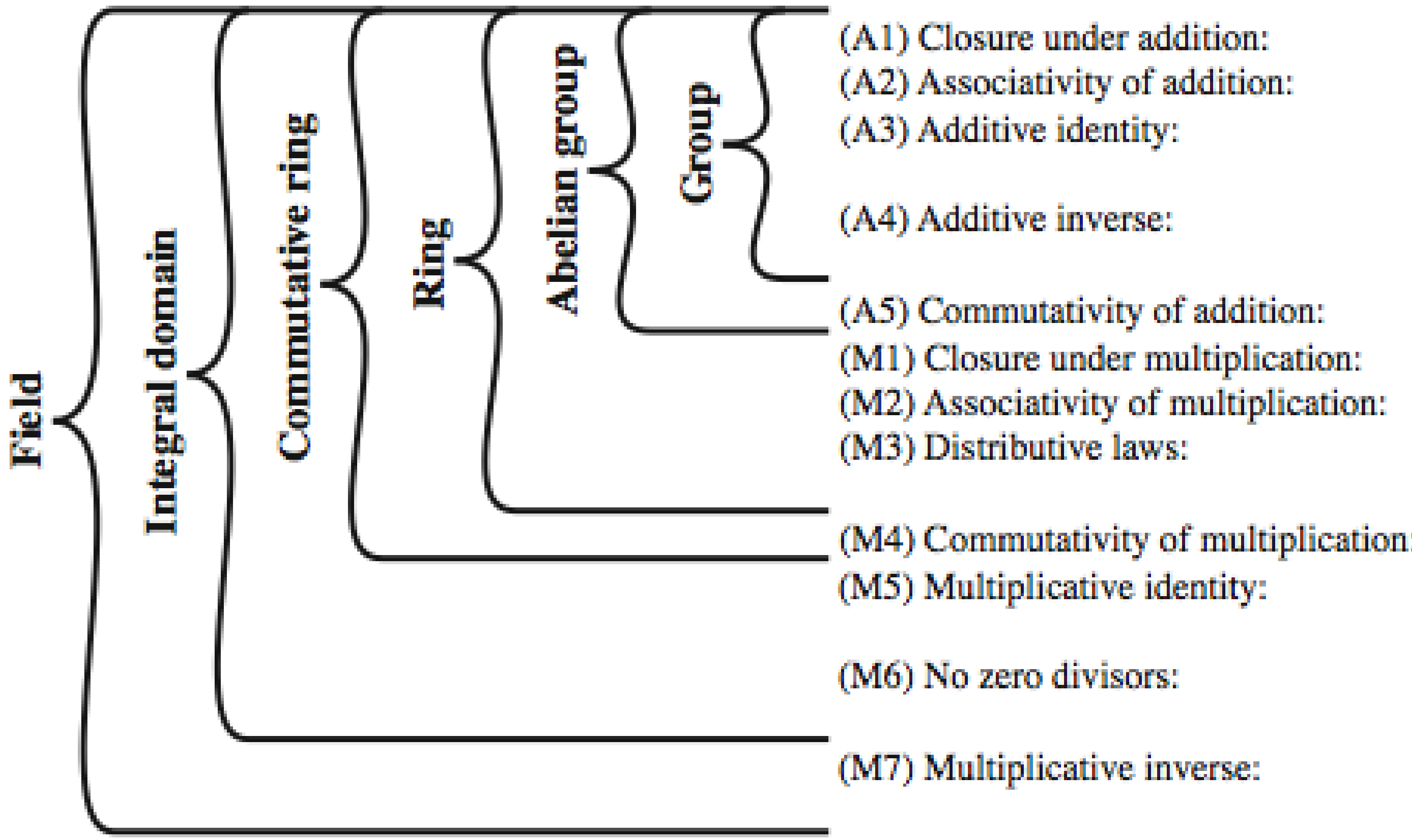
- We denote a Ring as {R,+,.}
- if multiplication operation is commutative, it forms a commutative ring

- if multiplication operation has an identity and no zero divisors, it forms an integral domain

Field

- a set of numbers with two operations which form:
  - abelian group for addition
  - abelian group for multiplication (ignoring 0)
  - F has multiplicative reverse
    - For each a in F other than 0, there is an element b such that ab=ba=1
- We denote a Field as {F,+,.}
- Examples of fields: rational numbers, real numbers, complex numbers. Integers are NOT a field.
- have hierarchy with more axioms/laws
  - group -> ring -> field

Group, Ring, Field



Divides, Factor, Multiple

- Let $a,b \in \mathbf{Z}$ with $a \neq 0$.
- $3 \mid 12$
  - To specify when an integer evenly divides another integer
  - Read as "3 divides 12"

- Defn.: $a|b \equiv$ "*a divides b*" $:\equiv (\exists\, c \in \mathbf{Z}: b = ac)$
- "There is an integer *c* such that *c* times *a* equals *b*."
  - Example: $3 \mid -12 \Leftrightarrow$ True, but $3 \mid 7 \Leftrightarrow$ False.

- Iff *a* divides *b*, then we say *a* is a *factor* or a *divisor* of *b*, and *b* is a *multiple* of *a*.

Results on the divides operator

- If a | b and a | c, then a | (b+c)
  - Example: if 5 | 25 and 5 | 30, then 5 | (25+30)
- If a | b, then a | bc for all integers c
  - Example: if 5 | 25, then 5 | 25*c for all ints c
- If a | b and b | c, then a | c
  - Example: if 5 | 25 and 25 | 100, then 5 | 100

The Division "Algorithm"

- Theorem:
- Division Algorithm : Let a be an integer and *d* a positive integer.
- There are *unique* integers q and r, with $0 \leq r < d$, such that $a = dq+r$.

  - q : ***quotient***
  - r : ***remainder***
  - d : ***divisor***
  - a : ***dividend***

Modular arithmetic

- If *a* and *b* are integers and *m* is a positive integer, then
- *"a is congruent to b modulo m"* if *m* divides *a-b*
  - Notation: $a \equiv b \pmod{m}$
  - Rephrased: $m \mid a-b$
  - Rephrased: *a* mod *m* = *b* mod *m*
  - If they are not congruent: $a \not\equiv b \pmod{m}$
- Example: Is 17 congruent to 5 modulo 6?
  - Rephrased: $17 \equiv 5 \pmod{6}$
  - As 6 divides 17-5, they are congruent
- Example: Is 24 congruent to 14 modulo 6?
  - Rephrased: $24 \equiv 14 \pmod{6}$
  - As 6 does not divide 24-14 = 10, they are not congruent

Even even more on congruence

- *Theorem:* Let m *be a positive integer.*
  - If $a \equiv b \ (mod\ m)$ and $c \equiv d \pmod{m}$,
  - then $a+c \equiv (b+d) \pmod{m}$ and $ac \equiv bd \pmod{m}$

- Example
  - We know that 7 ≡ 2 (mod 5) and 11 ≡ 1 (mod 5)
  - Thus, 7+11 ≡ (2+1) (mod 5), or 18 ≡ 3 (mod 5)
  - Thus, 7*11 ≡ 2*1 (mod 5), or 77 ≡ 2 (mod 5)

Modular Arithmetic

- define **modulo operator** ***a mod n*** to be remainder when a is divided by n
- use the term **congruence** for: ***a ≡ b mod n***
  - when divided by *n*, a & b have same remainder
  - eg. ***100 ≡ 34 mod 11***
- b is called the **residue** of a mod n
  - since with integers can always write: ***a = qn + b***
- usually have ***0 <= b <= n-1***

-12 mod 7 ≡ -5 mod 7 ≡ 2 mod 7 ≡ 9 mod 7

Modulo 7 Example

...

-21	-20	-19	-18	-17	-16	-15
-14	-13	-12	-11	-10	-9	-8
-7	-6	-5	-4	-3	-2	-1
0	**1**	**2**	**3**	**4**	**5**	**6**
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	29	30	31	32	33	34

...

Modular Arithmetic Operations

- can do modular arithmetic with any group of integers: $Z_n = \{0, 1, \ldots, n-1\}$
  - Can perform addition & multiplication
  - Do modulo to reduce the answer to the finite set
- can do reduction at any point, ie
  - **a+b mod n = a mod n + b mod n**
- form a commutative ring for addition,with a multiplicative identity
  - if **(a+b)≡(a+c) mod n** then **b≡c mod n**
  - but **(ab)≡(ac) mod n** then **b≡c mod n** iff **a** is relatively prime to **n**

Modular Arithmetic Operations

1. [(a mod n) + (b mod n)] mod n = (a + b) mod n
2. [(a mod n) – (b mod n)] mod n = (a – b) mod n
3. [(a mod n) x (b mod n)] mod n = (a x b) mod n

e.g.

[(11 mod 8) + (15 mod 8)] mod 8 = 10 mod 8 = 2 (11 + 15) mod 8 = 26 mod 8 = 2

[(11 mod 8) – (15 mod 8)] mod 8 = –4 mod 8 = 4 (11 – 15) mod 8 = –4 mod 8 = 4

[(11 mod 8) x (15 mod 8)] mod 8 = 21 mod 8 = 5 (11 x 15) mod 8 = 165 mod 8 = 5

Modulo 8 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
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

(a) Addition modulo 8

Modulo 8 Multiplication

+	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

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 $w + z \equiv 0 \bmod n$

Greatest Common Divisor (GCD)

- a common problem in number theory
- *GCD (a,b)* of *a* and *b* is the largest number that divides evenly into both *a* and *b*
  - eg GCD(60,24) = 12
  - eg GCD(8,15) = 1
  - hence 8 & 15 are relatively prime

Euclid's GCD Algorithm

- an efficient way to find the GCD(a,b)
- uses theorem that:
  - *GCD(a,b) = GCD(b, a mod b)*
- **Euclid's Algorithm** to compute GCD(a,b):

```
A=a, B=b
  while B>0
     R = A mod B
     A = B, B = R
  return A
```

Example GCD(1970,1066)

1970 = 1 x 1066 + 904	gcd(1066, 904)
1066 = 1 x 904 + 162	gcd(904, 162)
904 = 5 x 162 + 94	gcd(162, 94)
162 = 1 x 94 + 68	gcd(94, 68)
94 = 1 x 68 + 26	gcd(68, 26)
68 = 2 x 26 + 16	gcd(26, 16)
26 = 1 x 16 + 10	gcd(16, 10)
16 = 1 x 10 + 6	gcd(10, 6)
10 = 1 x 6 + 4	gcd(6, 4)
6 = 1 x 4 + 2	gcd(4, 2)
4 = 2 x 2 + 0	gcd(2, 0)

Extended Euclidean Algorithm

- calculates not only GCD but x & y:

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

- useful for later crypto computations
- follow sequence of divisions for GCD but assume at each step i, can find x &y:

  $$r = ax + by$$

- at end find GCD value and also x & y
- if GCD(a,b)=1 these values are inverses

Finding Inverses

- can extend Euclid's algorithm:

```
EXTENDED EUCLID(m, b)
1. (A1, A2, A3)=(1, 0, m);
   (B1, B2, B3)=(0, 1, b)
2. if B3 = 0
   return A3 = gcd(m, b); no inverse
3. if B3 = 1
   return B3 = gcd(m, b); B2 = b^-1 mod m
4. Q = A3 div B3
5. (T1, T2, T3)=(A1 – Q B1, A2 – Q B2, A3 – Q B3)
6. (A1, A2, A3)=(B1, B2, B3)
7. (B1, B2, B3)=(T1, T2, T3)
8. goto 2
```

Galois Fields

- finite fields play a key role in cryptography
- can show number of elements in a finite field **must** be a power of a prime p^n known as Galois fields denoted $GF(p^n)$
- in particular often use the fields:
  - $GF(p)$
  - $GF(2^n)$

Galois Fields GF(p)

- GF(p) is the set of integers {0,1, … , p-1} with arithmetic operations modulo prime p
- Multiplicative inverse

For each $w \in Z_p$, $w \neq 0$, there exists a $z \in Z_p$ such that $w \times z \equiv 1 \bmod p$

Modular Polynomial Arithmetic

- can write any polynomial in the form:
  - $f(x) = q(x)\,g(x) + r(x)$
  - can interpret $r(x)$ as being a remainder
  - $r(x) = f(x) \bmod g(x)$
- if have 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 field