CS557: Cryptography

Elementary Number Theory-III

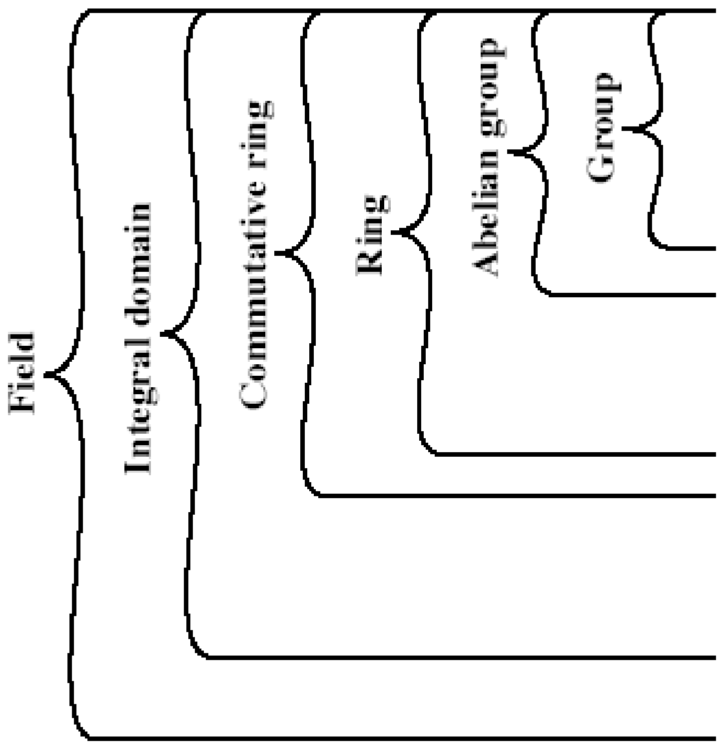
S. Tripathy
IIT Patna

Previous Class

- Elementary Number Theory
  - GCD
    - Euclidean Algorithm.
  - Group and Field

Field

- **a set of numbers with two operations: (F,+,.)**
  - **abelian group for + operation**
  - **abelian group for . operation (ignoring 0)**
  - **ring**



(A1) Closure under addition:	If a and b belong to S, then $a + b$ is also in S
(A2) Associativity of addition:	$a + (b + c) = (a + b) + c$ for all a, b, c in S
(A3) Additive identity:	There is an element 0 in R such that $a + 0 = 0 + a = a$ for all a in S
(A4) Additive inverse:	For each a in S there is an element $-a$ in S such that $a + (-a) = (-a) + a = 0$
(A5) Commutativity of addition:	$a + b = b + a$ for all a, b in S
(M1) Closure under multiplication:	If a and b belong to S, then ab is also in S
(M2) Associativity of multiplication:	$a(bc) = (ab)c$ for all a, b, c in S
(M3) Distributive laws:	$a(b + c) = ab + ac$ for all a, b, c in S $(a + b)c = ac + bc$ for all a, b, c in S
(M4) Commutativity of multiplication:	$ab = ba$ for all a, b in S
(M5) Multiplicative identity:	There is an element 1 in S such that $a1 = 1a = a$ for all a in S
(M6) No zero divisors:	If a, b in S and $ab = 0$, then either $a = 0$ or $b = 0$
(M7) Multiplicative inverse:	If a belongs to S and a 0, there is an element a^{-1} in S such that $aa^{-1} = a^{-1}a = 1$

1. All groups satisfy properties _,_,_...
2. A Ring satisfies the properties……
3. Field satisfies the properties……

$$\mathbb{Q}\sqrt{3} = \{ a + b\sqrt{3} \mid a, b \in \mathbb{Q} \}$$

Modular Arithmetic

- is 'clock arithmetic'
- uses a finite number of values, and loops back from either end
- x Ξ y mod n
- i.e, x is congruent to y mod n, if n divides (x-y).
- Equivalently, x and y have the same remainder when divided by n.
- Example: $23 \equiv 5 (\text{mod} 9)$
- modular arithmetic is when do addition & multiplication and modulo reduce answer
  - (a+b) mod n = [a mod n + b mod n] mod n
- We work in Zn = {0, 1, 2, …, n-1}, the ring of integers modulo m with binary operators + and * defined modulo n.
- Example: Z9 ={0,1,2,3,4,5,6,7,8}

Modular Arithmetic

Def : $m \in N^+$, $a \in Z$.

a mod m → the remainder of a divided by m.

- Ex:
  - 17 mod 5 = 2
  - -133 mod 9 = 2.

Def : $a,b \in Z$, $m \in N^+$.

$a \equiv b \pmod{m}$ means $m \mid (a-b)$.

  - i.e., a and b have the same remainder when divided by m.
  - i.e., a mod m = b mod m
  - we say a is congruent to b (module m).
- Ex:
  - $17 \equiv 5 \pmod{6}$?
  - $24 \equiv 14 \pmod{6}$?

Congruences

- **Examples:**
- Is it true that $46 \equiv 68 \pmod{11}$?
  - Yes, because $11 \mid (46 - 68)$.
- Is it true that $46 \equiv 68 \pmod{22}$?
  - Yes, because $22 \mid (46 - 68)$.
- For which integers z it is true that $z \equiv 12 \pmod{10}$?
  - It is true for any $z \in \{\ldots, -18, -8, 2, 12, 22, 32, \ldots\}$

- **Theorem:** Let m be a positive integer. The integers a and b are congruent modulo m if and only if there is an integer k such that $a = b + km$.

Some More Definitions: Common divisors

- The common divisors of two numbers x, y are the numbers z such that $z|x$ and $z|y$

- x and y are relatively prime if they have no common divisors, other than 1
  - 9 and 14 are relatively prime
  - 9 and 15 are not relatively prime

- Equivalently, x and y are relatively prime if $\gcd(x,y) = 1$

Euler's totient function

- Given positive integer n, Euler's totient function is the number of positive numbers less than n that are relatively prime to n. $\Phi(n)$

Fact: If p is prime then {1,2,3,…,p-1} are relatively prime to p. $\Phi(p) = p-1$

- If p and q are prime and n=pq then $\Phi(n) = (p-1)(q-1)$

  $\Phi(p^m) = (p-1)(p^{m-1})$
- Fermat's little Theorem: If a is relatively prime to n then $a^{\Phi(n)} = 1 \bmod n$
- $a^{p-1} = 1 \bmod p$

Addition modulo operation

- Addition is well-defined:
- If $x \equiv y \bmod n$ and $x_1 \equiv y_1 \bmod n$ then

  $x+x_1 \equiv (y+y_1) \bmod n$
- $14 \equiv 5 \bmod 9$ and $11 \equiv 2 \bmod 9$.
- $25 \equiv 7 \bmod 9$
- 0 is the additive identity in Zm:
  - $x + 0 \equiv x \pmod{m} \equiv 0 + x \pmod{m}$
- Additive inverse: Every element has unique additive inverse. $4 + 5 = 0 \bmod 9$.
  - 4 is additive inverse of 5.

- Complexity?

Multiplication in Zm:

- Multiplication is well-defined:
- If $x \equiv y \bmod n$ and $x_1 \equiv y_1 \bmod n$ then
- $X * x_1 \equiv (y * y_1) \bmod n$
- $12 \equiv 3 \bmod 9$ and $20 \equiv 2 \bmod 9$.
- $240 \equiv 6 \bmod 9$.
- 1 is the multiplicative identity in Zn

- Complexity?

Unique representation system mod 4

Finite set S = {0, 1, 2, 3}

+ and * defined on S:

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

*	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

Multiplicative inverses in Zn

- Multiplicative inverse –
  - SOME, but not ALL elements have unique multiplicative inverse.
  - In Z9:
    - 3*0=0, 3*1=3, 3*2=6, 3*3=0, 3*4=3, 3*5=6, …, so 3 does not have a multiplicative inverse.
    - What about 4,

      4*2=8, 4*3=3, 4*7 =1 i.e, $4^{-1} = 7$

  - In Zn, x has a multiplicative inverse if and only if x and n are relatively prime.

    E.g., in Z_9, 3 (does not have) but 4 (has =7)
  - If gcd(x,m) = 1, as y varies, y*x takes on m distinct values, so for some value, y*x=1mod m.

Theorem (uniqueness of inverse)

- $m > 0$, $\gcd(a,m) = 1$. Then $\exists\, b \in Z$ s.t.
  - 1. $ab \equiv 1 \pmod{m}$
  - 2. if $ab \equiv ac$ $[\equiv 1]$ $\Rightarrow$ $b \equiv c \pmod{m}$.

Pf: 1. $\gcd(a,m) = 1$. Then $\exists\, b,t$ with $ba + tm = 1$.
since $ab - 1 = (-t)\, m$, $ab \equiv 1 \pmod{m}$.

2. Since $\gcd(a,m)=1$, we can divide a from both sides.

Note: Above theorem means that the inverse of a mod m uniquely exists (and hence is well defined) if a and m are relatively prime.

Fermat's theorem to compute Inverse

Thm: Let p be a prime

$$\forall\ x \in (Z_p)^* : \qquad x^{p-1} = 1 \text{ in } Z_p$$

So: $x \in (Z_p)^* \Rightarrow x \cdot x^{p-2} = 1 \Rightarrow x^{-1} = x^{p-2}$ in Z_p

Another way to compute inverses, but less efficient

Example: p=5. $3^4 = 81 = 1$ in Z_5

What is the inverse?

- Thanks