Computer and Network Security

Lecture 6

Some math…

Outline

- Groups
  - Abelian
  - Cyclic
  - Generator
  - Group order
- Rings
- Fields
- Theorems
- Euclidian Algorithm
- CRT

Groups

- A non-empty set G and operator @, (G,@) is a **group** if
  - CLOSURE
    - $\forall$ x, y $\in$ G: x @ y $\in$ G
  - ASSOCIATIVITY
    - $\forall$ x, y, z $\in$ G: (x @ y) @ z = x @ (y @ z)
  - IDENTITY
    - $\exists$ i $\in$ G, such that, $\forall$ x $\in$ G: i @ x = x and x @ i = x
  - INVERSE
    - $\forall$ x $\in$ G, $\exists$ x^{-1} $\in$ G, such that: x^{-1} @ x = i = x @ x^{-1}

- A group (G,@) is **abelian** if
  - COMMUTATIVITY
    - $\forall$ x, y $\in$ G: x @ y = y @ x

Groups

- g $\in$ G is a **group generator** of group (G,@) if
  - G= {g^x| x integer}
  - G = <g>

- A group (G,@) is **cyclic** if a group generator exists

- The **order** of group (G,@) is the size of set G
  - |G| or #{G} or ord(G)

- A group (G,@) is **finite** if ord(G) is fixed

Ring and Fields

- A triple (R,+,*) is a **ring** if
  - (R,+) is an abelian group
  - CLOSURE
    - $\forall$ x, y $\in$ R: x * y $\in$ R
  - ASSOCIATIVITY
    - $\forall$ x, y, z $\in$ R: (x * y) * z = x * (y * z)
  - IDENTITY
    - $\exists$ i $\in$ R, such that, $\forall$ x $\in$ R: i * x = x and x * i =
  - DISTRIBUTION
    - $\forall$ x,y,z $\in$ R: (x + y) * z = x * z + y * z

Ring and Fields

- A triple (F,+,*) is a **field** if
  - (F,+,*) is a ring
  - INVERSE
    - $\forall$ x $\in$ R, $\exists$ x^{-1} in R, such that: x^{-1} * x = i = x * x^{-1}

Modular Arithmetic

- Z = {…, -3, -2, -1, 0, 1, 2, 3, …}
- Z_n = {0, 1, 2, . . . , n-1}
  - Example: Z_5 = {0, 1, 2, 3, 4}
- Do the Additive and Multiplicative Identity and Inverse Properties of real numbers hold up for Z_n?
- Does it depend on **n**?

Modular Arithmetic

- The Additive Identity Property
  - a + 0 = a
- The Multiplicative Identity Property
  - a * 1 = a

Additive inverse property

- a + **-a** = 0
  - What is the meaning of -a in Z_n?
    - Z_{12} = {0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11}
    - There are no negative numbers
    - Can we find numbers to add to a given element in Z_{12} such that the sum will be zero?

Addition table in Z_{12}

Plus	0	1	2	3	4	5	6	7	8	9	10	11
0	**0**	1	2	3	4	5	6	7	8	9	10	11
1	1	2	3	4	5	6	7	8	9	10	11	**0**
2	2	3	4	5	6	7	8	9	10	11	**0**	1
3	3	4	5	6	7	8	9	10	11	**0**	1	2
4	4	5	6	7	8	9	10	11	**0**	1	2	3
5	5	6	7	8	9	10	11	**0**	1	2	3	4
6	6	7	8	9	10	11	**0**	1	2	3	4	5
7	7	8	9	10	11	**0**	1	2	3	4	5	6
8	8	9	10	11	**0**	1	2	3	4	5	6	7
9	9	10	11	**0**	1	2	3	4	5	6	7	8
10	10	11	**0**	1	2	3	4	5	6	7	8	9
11	11	**0**	1	2	3	4	5	6	7	8	9	10

Additive inverse property

- a + **-a** = 0
  - What is the meaning of -a in Z_{12}?
    - a = 5 → -a = 7
      - 5 + 7 = 0
    - a = 3 → -a = 9
      - 3 + 9 = 0
  - Then **-a** can be translated as **(n – a)**

Multiplicative Inverse Property

- a * **1/a** = 1
  - What is the meaning of 1/a in Z_n?
    - Z_{12} = {0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11}
    - There are no fractions
    - Can we find numbers to multiply a given element in Z_{12} such that the product will be one?
    - We know that
      - 1/a = k → k * a = 1

Multiplication Table in Z_{12}

Times	0	1	2	3	4	5	6	7	8	9	10	11
0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	**1**	2	3	4	5	6	7	8	9	10	11
2	0	2	4	6	8	10	0	2	4	6	8	10
3	0	3	6	9	0	3	6	9	0	3	6	9
4	0	4	8	0	4	8	0	4	8	0	4	8
5	0	5	10	3	8	**1**	6	11	4	9	2	7
6	0	6	0	6	0	6	0	6	0	6	0	6
7	0	7	2	9	4	11	6	**1**	8	3	10	5
8	0	8	4	0	8	4	0	8	4	0	8	4
9	0	9	6	3	0	9	6	3	0	9	6	3
10	0	10	8	6	4	2	0	10	8	6	4	2
11	0	11	10	9	8	7	6	5	4	3	2	**1**

Multiplicative Inverse Property

- a * **1/a** = 1
  - Only {1, 5, 7, 11} have inverses
    - 5 and 7 are the inverses of each other
    - Both 1 and 11 are their own inverses
    - Why don't the other numbers have inverses?

Multiplicative Inverse Property

- a * **1/a** = 1
  - For n = 11, 10, 9, 8, 7, 6, 5,…
    - Which numbers have inverses and which do not?
    - Is there a pattern to this?
    - Is there a number in every mod that has a multiplicative inverse (aside from 1)?
    - Let's look…

Multiplication Table in Z_{11}

Times	0	1	2	3	4	5	6	7	8	9	10
0	0	0	0	0	0	0	0	0	0	0	0
1	0	**1**	2	3	4	5	6	7	8	9	10
2	0	2	4	6	8	10	**1**	3	5	7	9
3	0	3	6	9	**1**	4	7	10	2	5	8
4	0	4	8	**1**	5	9	2	6	10	3	7
5	0	5	10	4	9	3	8	2	7	**1**	6
6	0	6	**1**	7	2	8	3	9	4	10	5
7	0	7	3	10	6	2	9	5	**1**	8	4
8	0	8	5	2	10	7	4	**1**	9	6	3
9	0	9	7	5	3	**1**	10	8	6	4	2
10	0	10	9	8	7	6	5	4	3	2	**1**

Multiplication Table in Z_{10}

Times	0	1	2	3	4	5	6	7	8	9
0	0	0	0	0	0	0	0	0	0	0
1	0	**1**	2	3	4	5	6	7	8	9
2	0	2	4	6	8	0	2	4	6	8
3	0	3	6	9	2	5	8	**1**	4	7
4	0	4	8	2	6	0	4	8	2	6
5	0	5	0	5	0	5	0	5	0	5
6	0	6	2	8	4	0	6	2	8	4
7	0	7	4	**1**	8	5	2	9	6	3
8	0	8	6	4	2	0	8	6	4	2
9	0	9	8	7	6	5	4	3	2	**1**

Multiplication Table in Z_9

Times	0	1	2	3	4	5	6	7	8
0	0	0	0	0	0	0	0	0	0
1	0	**1**	2	3	4	5	6	7	8
2	0	2	4	6	8	**1**	3	5	7
3	0	3	6	0	3	6	0	3	6
4	0	4	8	3	7	2	6	**1**	5
5	0	5	**1**	6	2	7	3	8	4
6	0	6	3	0	6	3	0	6	3
7	0	7	5	3	**1**	8	6	4	2
8	0	8	7	6	5	4	3	2	**1**

Multiplication Table in Z_8

Times	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**

Multiplication Table in Z_7

Times	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**

Multiplication Table in Z_6

Times	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	**1**	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	**1**

Multiplication Table in Z_5

Times	0	1	2	3	4
0	0	0	0	0	0
1	0	**1**	2	3	4
2	0	2	4	**1**	3
3	0	3	**1**	4	2
4	0	4	3	2	**1**

Multiplication Inverse Property Summary

Z_n	Have Inverse	Don't Have Inverse
12	1, 5, 7, 11	0, 2, 3, 4, 6, 8, 9, 10
11	1, 2, 3, 4, 5, 6, 7, 8, 9, 10	0
10	1, 3, 7, 9	0, 2, 4, 5, 6, 8
9	1, 2, 4, 5, 7, 8	0, 3, 6
8	1, 3, 5, 7	0, 2, 4, 6
7	1, 2, 3, 4, 5, 6	0
6	1, 5	0, 2, 3, 4
5	1, 2, 3, 4	0

Multiplication Inverse Property Summary

Z_n	Have Inverse	Don't Have Inverse
12	**1**, 5, 7, **11**	**0**, 2, 3, 4, 6, 8, 9, 10
11	**1**, 2, 3, 4, 5, 6, 7, 8, 9, **10**	**0**
10	**1**, 3, 7, **9**	**0**, 2, 4, 5, 6, 8
9	**1**, 2, 4, 5, 7, **8**	**0**, 3, 6
8	**1**, 3, 5, **7**	**0**, 2, 4, 6
7	**1**, 2, 3, 4, 5, **6**	**0**
6	**1**, **5**	**0**, 2, 3, 4
5	**1**, 2, 3, **4**	**0**

Multiplication Inverse Property Summary

- **0** never has an inverse
  - The Multiplicative Property of Zero holds
- **1** is always its own inverse
- **-1** in the form of **(n – 1)** is also always its own inverse

Multiplication Inverse Property Summary

Z_n	Have Inverse	Don't Have Inverse
12	1, **5, 7,** 11	0, **2, 3, 4, 6, 8, 9, 10**
11	1**, 2, 3, 4, 5, 6, 7, 8, 9,** 10	0
10	1, **3, 7**, 9	0, **2, 4, 5, 6, 8**
9	1, **2, 4, 5, 7,** 8	0, **3, 6**
8	1, **3, 5,** 7	0, **2, 4, 6**
7	1, **2, 3, 4, 5,** 6	0
6	1, 5	0, **2, 3, 4**
5	1, **2, 3,** 4	0

Multiplication Inverse Property Summary

- The numbers that have inverses in Z_n are **relatively prime** to n
  - That is: GCD(x, n) = 1
- The numbers that do **NOT** have inverses in Z_n have **common prime factors** with n
  - That is: GCD(x, n) > 1

Multiplication Inverse Property Conclusion

- The results have implications for division:
  - Some divisions have no answers
    - 3 * x = 2 mod 6 has no solutions => 2/3 has no equivalent in Z_6
  - Some division have multiple answers
    - 2 * 2 = 4 mod 6 => 4/2 = 2 mod 6
    - 2 * 5 = 4 mod 6 => 4/2 = 5 mod 6
  - Only numbers that are **relatively prime** to n will be uniquely divisible by all elements of Z_n
    - Denote Z^*_n = { x | GCD(x, n)=1}
  - If n is prime, 1≤ x ≤ n-1 are **all relatively prime** to n
    - Then Z^*_n = {1, 2, …, n-1}

Subgroups

- (H,@) is a **subgroup** of (G,@) if
  - $H \subseteq G$
  - (H,@) is a group

Example

- (G,*), $G = Z^*_7$ = {1,2,3,4,5,6} abelian group
- H = {1,2,4} abelian subgroup
  - H is closed under multiplication mod 7
  - 1 is still the identity
  - 1 is 1's inverse, 2 and 4 are inverses of each other
  - associativity holds
  - commutativity holds

Order of an element

- Let x ∈ G, (G,*) finite integer group
- ord(x)
  - the smallest positive number k such that x^k= 1
- Example:
  - (Z^*_7, *)
    - ord(1) = 1 because 1^1 = 1
    - ord(2) = 3 because 2^3 = 8 = 1
    - ord(3) = 6 because 3^6 = 729 = 23 =1
    - ord(4) = 3 because 4^3 = 64 = 1
    - ord(5) = 6 because 5^6 = 15625 = 1
    - ord(6) = 2 because 6^2 = 36 = 1

Other facts from number theory

- Euler's totient function:
  - ϕ(n) = number of positive integers ≤n and coprime with n
    - n prime → ϕ(n) = n-1
    - GCD(m,n) = 1, then ϕ(mn) = ϕ(m) ϕ(n)
      - m, n prime → ϕ(mn) = (m-1)(n-1)
- ord(G^*_n) = largest order or any x ∈ G = ϕ(n)
- Lagrange's Theorem:
  - Suppose G is a multiplicative group of order s and g∈G, then the ord(g) divides s
  - Corollary:
    - If g ∈ Z^*_n → $g^{\phi(n)}$ = 1 mod n
    - Indeed
      - ord(g) = ord(Z^*_n)/k = ϕ(n) / k
      - $x^{\phi(n)} = x^{\phi(n)/k} = 1^{1/k}$ = 1 mod n
- Fermat's Little Theorem:
  - Let n be a prime, any integer x satisfies
    - x^n = x mod n
    - any integer x not divisible by n satisfies a^{n-1} = 1 mod n

Finding Inverses in Z_n

- Does x has inverse in Z_n?
  - That is GCD(x, n)=1?
  - Euclidean Algorithm
    - Euclid's Elements around 300 BC
    - Computes GCD(x, n)
- Which is the inverse of x in Z_n?
  - Extended Euclidean Algorithm

Euclidean Algorithm

- Inverse of 15 in Z_{26}
- Euclidean Algorithm to compute GCD(26, 15)
  - 26 = 1 * 15 + 11
  - 15 = 1 * 11 + 4
  - 11 = 2 * 4 + 3
  - 4 = 1 * 3 + 1
  - 3 = 3 * 1 + 0

Extended Euclidean Algorithm

- Inverse of 15 in Z_{26}
  - GCD(26, 15) = 1 → Inverse must exist
  - Set GCD(26, 15) as a linear combination of 26 and 15
    - 1 = x * 26 + y * 15
  - Work backward

Extended Euclidean Algorithm

- 26 = 1 * 15 + 11 => 11 = 26 – (1*15)
- 15 = 1 * 11 + 4 => 4 = 15 – (1*11)
- 11 = 2 * 4 + 3 => 3 = 11 – (2*4)
- 4 = 1 * 3 + 1 => 1 = 4 – (1*3)

Step 1) 1 = 4 – (1 * 3) = 4 – 3

Step 2) 1 = 4 – (11 – (2 * 4)) = 3 * 4 - 11

Step 3) 1 = 3 * (15 – 11) – 11 = 3 * 15 – 4 * 11

Step 4) 1 = 3 * 15 – 4(26 – (1*15)

Step 5) 1 = 7 * 15 – 4 * 26 = 105 – 104

Extended Euclidean Algorithm

- Inverse of 15 in Z_{26}?
  - 1 = 7 * 15 – 4 * 26
  - 1 = 7 * 15 mod 26
  - 7 is the inverse of 15 in mod 26
  - 7*15 = 105 = 1 mod 26

Chinese Reminder Theorem (CRT)

- Assume $\{m_1, \ldots, m_n\}$ pairwise coprime.
  - For any $a_1, \ldots, a_n$ the system of congruencies

$$x \equiv a_1 \; mod \; m_1$$
$$\ldots$$
$$x \equiv a_n \; mod \; m_n$$

  - Has unique solution

$$x = \sum_{i=1}^{n} a_i \left(\frac{M}{m_i} \right) y_i \; mod \; M$$

where :

$$M = m_1 * \ldots * m_n$$

$$y_i = \left(\frac{M}{m_i} \right)^{-1} mod \; m_i$$

  - Used in RSA to speed-up computation