Lecture 2 Modular Arithmatics :
Shift Cipher/Ceaser Cipher
Affine Cipher

Finite Sets :-
Eg of finite sets in real life are :- Clock, it is very easy to find finite sets in Circle/Bounded Structure.

12 hr + 20 = 32 ~ Actually 32 mod 24.

Mode Operator : remainder operator

2.4.3 The integers modulo n Let n be a positive integer.

- **2.110 Definition** If a and b are integers, then a is said to be *congruent to* b *modulo* n, written a ≡ b (mod n), if n divides (a−b). The integer n is called the *modulus* of the congruence.

- **2.111 Example** (i)24≡9 (mod5)since24−9=3·5.
  (ii)−11≡17 (mod 7)since−11−17=−4·7.

- **2.112 Fact** (*properties of congruences*) For all a, a1, b, b1, c ∈ Z, the following are true.
  - a ≡ b (mod n) if and only if a and b leave the same remainder when divided by n.
  - (*reflexivity*) a ≡ a (mod n).
  - (*symmetry*) If a ≡ b (mod n) then b ≡ a (mod n).
  - (*transitivity*)If a≡b (mod n) and b≡c (mod n),then a≡c (mod n)
  - If a ≡ a1 (mod n) and b ≡ b1 (mod n),then a+b ≡ a1 +b1 (mod n)and ab ≡ a1b1 (mod n). —> as same reminder so if you solve as a = k*n + r and b = q*n + r then a*b mod n -> result into r^2.

Eg,
1. say a = 13, m = 9 what is r ? r = 4.
2. a - r = 13-4 = 9, 9 is divisible by m so definition holds.

1. Say a = 42, m=9 what is r ?
2. r = 6 if q = 4
3. But q = 3 then r = 15
4. and above all holds the rule of m | a-r
5. **So reminder is not unique.**

Equivalence Classes :-
Eg :- a = 12, m = 5
1. 12 congruent 2 mod 5
2. 12 congruent 7 mod 5.

3. 12 congruent -3 mod 5

Def of set :-
{ -3, 2 , 7 , 12} => modulo 5 equivalence class
All the modulo 5 equivalence classes :-

1. {.. , -10, -5, 0, 5, 10, 15, …} => A
   1. Infinite numbers will be there.
   2. This set doesn't contain all the integers.
2. {.. , -9, -4, 1, 6, 11, 16, …} => B
3. {.., -8, -3, 2, 7, 12, 17, …} => C
4. {.., -7, -2, 3, 8, 13, 18, …} => D
5. {.., -6, -1, 4, 9, 14, 19, …} => E

Now all the above classes combines contains all the integers.

In crypto we reduce the infinite numbers to something similar to above, finite equivalence classes. As equivalence classes have property, ie all the equivalence class members behave similar.

Eg. 13*16 - 8 => 208 - 8 => 200 congruent 0 mod 5 ie r = 0, m = 5
Lets do arithmetics with A,B,C,D,E :-
D.B - D => as per definition all members of class behave equivalent so we pick some number from D class (**Smaller**) say 3, B we can choose 1 so 3*1-3 => 0

Important application :
Majorly Asymmetric encryption depends on modular arithmetics. Always we do exponential computations.
Eg. 3^8 mod 7, generally it is used on most of the browsers.

Rings :- Algebraic view on modular arithmetic :
Def => the integer ring Zm consists of

1. Set Zm = {0,1,….,m-1}
2. a+b congruent to c mod m
3. a*b congruent to d mod m

Addition and multiplication in ring are associative.
0 is the neutral element w.r.t addition in rings and 1 w.r.t multiply
But there might be cases in future where neural element is something else.

4. Additive Inverse (a) + -a = 0
5. Multiplicative inverse => a*(a inverse) congruent to 1 mod m

Say m = 9, a = 2 now we need to find the inverse of a ?
2 table 2,4,6,8,10 as we see 10 mod 9 is 1 so 2*(5), means 5 is the multiplicative inverse.

Say m = 9, a = 6 , find the multiplicative inverse.
{0,6,12,18,24}, it is not possible, there is an easy test to check of multiplicative inverse exists ? Using GCD.

Find gcd(6,9) ==> 3, gcd(2,9) ==> 1
So the rule is if GCD of module and number is 1 then there is an inverse.

Question : Proof the above GCD way ?
In a ring we only have +,-,* but not always divide.
In a group, which is smallest element set, where only + and - are there.

Shift Cipher =>
2 Attacks:-
1. **Frequency Attack.**
2. **Brute force Attack.**

Afine Cipher =>
1. Divide keyspace in 2 parts k = (a,b)
2. Encryptions => Y congruent a*x + b mod 26
3. Decryption => Y - b congruent a*x mod 26
4. (a inverse) * Y -b mod 26 = x
5. #key space => number of b's —> 26 as it is just shift. Number of a's —> gcd(a,26) —> 1 => [3,5,7…]
6. #key space of a = 12, total key space is 12 * 26
7. Same as above attacks holds.