Week 5 Modular Arithmetic Lecture Note

Notebook:	Computational Mathematics		
Created:	2020-04-21 2:48 PM	**Updated:**	2020-05-05 5:27 PM
Author:	SUKHJIT MANN		

Cornell Notes	**Topic:** Modular Arithmetic	Course: BSc Computer Science Class: Computational Mathematics[Lecture] Date: May 05, 2020

Essential Question:

What are the operations performed with congruent numbers and their application to the field of computer science?

Questions/Cues:

- What is modular arithmetic?
- What is general way of writing congruence between two numbers?
- What is the more formal definition of modular arithmetic?
- How do you perform modular arithmetic on negative numbers?

Notes

- Modular Arithmetic = A way to classify integers, in a sense it is an arithmetic over integers; first introduced by mathematician and physicist Carl Friedrich Gauss
  - used in comp sci when dealing with long numbers, simplifying operation with long numbers
  - At the core of modular arithmetic is the idea of congruence between integers
  - Two numbers a & b are congruent, for example "mod 2" or modulus 2 if when they are divided by 2, they have the same remainder
- Congruency (general) =

$$a \overset{congruent}{\equiv} b \pmod{k} \Leftrightarrow a = nk + R, b = mk + R$$

  - Where R is the remainder and a, b, k are generic integers

- Example $3 \equiv 5 (mod 2)$
  since $3/2=1$ with R=1 $5/2=2$ with R=1

- Familiar example: the clock,

  if now it is 8 AM after 7 hs it will be 15 or 3 PM (it is "*mod 12*")

  $\rightarrow$ $15 \equiv 3$ (*mod 12*)

  since $15/12=1$ with R=3 $3/12=0$ with R=3

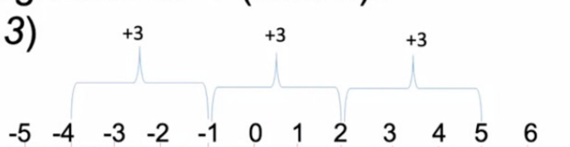
  - Modular Arithmetic (formal) = $\mathrm{mod}\ k$ is mapping by congruence all integers to the subset of non-negative integers smaller than k to which all other integers can be shown to be congruent to that is: $Min_k = \{0,1,2,...k-1\}$
    - The subset is referred to as the minimal subset
      - This subset is special because it is made of integers that when they are divided by the modulus k they coincide with the remainder
    - For example, modulus 12 or $\mathrm{mod}\ 12$, the minimal subset is $Min_{12} = \{0,1,2,3,4,5,6,7,8,9,10,11\}$ and no other integers can be shown to be congruent to the elements of this minimal subset. So if you have a positive integer, you just divide by k, and take the remainder & that remainder will give you the element of the minimal subset to which that number is congruent to

- With negative integers when we divide by *k* we need to get a <u>non-negative remainder</u>
  Ex: -17 *mod 12*
  you cannot do $-17/12= -1$ with R=-5 negative (wrong)
  but $-17/12 = -2$ with R=7 positive
  $\rightarrow -17 \equiv 7$ (*mod 12*)

- Other way: -17 reverse sign $\rightarrow 17 \equiv 5$ (*mod 12*) reverse sign to 5 and add *k(=12)* $-5+12=7$ $\rightarrow -17 \equiv 7$ (*mod 12*)

- Other example -12(*mod 5*) $\rightarrow 12 \equiv 2$(*mod 5*) $\rightarrow -2+5=3$
  $\rightarrow -12 \equiv 3$ (*mod 5*)

- What are the integers congruents to -1 (*mod 3*)?
  $...\equiv -4 \equiv -1 \equiv 2 \equiv 5 \equiv ...$(*mod 3*)

since $a \equiv b$ (*mod 3*) $\Leftrightarrow$ $a=n3+R$ and $b=m3+R$
$\rightarrow a-b= (n-m)3$

Examples

- 23 what is the smallest congruent number *mod 5*?
  23/5 =4 with R=3 → $23 \equiv 3 \pmod 5$

- 1101024 what is the smallest congruent number *mod 5*?
  1101024=1101020+4 →R=4 → $1101024 \equiv 4 \pmod 5$

- -2367(*mod 5*) ? → 2367/5=473 R=2 -2+5=3
  → $-2367 \equiv 3 \pmod 5$

Summary

In this week, we learned about what modular arithmetic is and how it can be performed on both positive and negative numbers.