Week 7
Term 1
2014

Learning Brief

SME1: Number Theory, Graphs and Networks

Goals

This is a busy week, manage your time wisely, and don't wait but see me if you are stuck on any concept.

By the end of this week, you should be able to:

- Use integers and their properties to understand basic principles on divisibility, greatest common divisors (gcd), least common multiples (lcm) and modular arithmetic
- Use Euclidean Algorithm to find the gcd of a pair of numbers
- Recognise congruent elements
- Find the residues in a modular system
- Construct Cayley's table and appreciate the importance the modular system
- USE CLASSPAD TO COMPUTE GCD, AND PERFORM MODULAR ARITHMETIC

Theoretical Components

1. Go through the notes and examples on Number Theory (pdf version available on cLc under 'Learning Brief' folder.
2. Divisibility RULES:
   http://www.youtube.com/watch?v=i16N01IdIhk&feature=topics

   http://www.youtube.com/watch?v=y1rVfa1nhjw

   http://www.youtube.com/watch?v=P5oHmgB4Nfs&feature=channel
3. Euclidean Algorithm for gcd:
   http://www.youtube.com/watch?v=fwuj4yzoX1o
4. Modular Arithmetic Notes & Examples & Exercises:
   http://www.dsert.kar.nic.in/textbooksonline/Text%20book/English/class%20x/maths/English-Class%20X-Maths-Chapter06.pdf

Practical Components

Attempt the questions from Exercises in the pdf file available under '4'.

Read the notes below, and answer the questions that follow.

Quiz

No Quiz this week.

Forum

On cLc.
The Math Book from Hell had the following rather unrealistic fraction question: What is the sum of 1/54 and 1/72 of a kilometre? Rodney sensed that 54 x 72 (3888) was not the lowest common denominator and that using it would mean a lot of extra work.
(a) How could the lowest common denominator for 1/54 and 1/72 be found?
(b)What is the LCM of these fractions?

Investigation

The Sieve of Eratosthenes
How many prime numbers are there from 1 to 100? The following procedure is a relatively simple way of identifying the primes to 100.
1. Put a single slash (/) through the 1 block with a blue crayon or colored pencil. One is special:
It is the unit.
2. Circle 2 in orange. Then cross out with red all other numbers in the chart divisible by 2.
(Another way of saying this is: Cross out all numbers in the chart that are multiples of 2. It may help some children to have them count by twos.)
3. Circle in orange the next prime number: 3. With red, cross out any other multiple of 3 that has not already been crossed out. (It may help some children to count by threes and cross out any of these numbers not already crossed out.)
4. Circle in orange the next prime number: 5.
With red, cross out any other multiple of 5 that has not already been crossed out. It may help some children to encourage them to count by fives and cross out any numbers not already crossed out.)
5. Continue in this manner until all numbers are circled in orange (the primes) or crossed out in red (the composites). Note for what prime number you did not have to cross out any multiples to 100. Why was it unnecessary to cross out any numbers for this prime? Will it be necessary to check for multiples of the remaining primes or can you simply circle in orange all remaining numbers at this point?

91	92	93	94	95	96	97	98	99	100
81	82	83	84	85	86	87	88	89	90
71	72	73	74	75	76	77	78	79	80
61	62	63	64	65	66	67	68	69	70
51	52	53	54	55	56	57	58	59	60
41	42	43	44	45	46	47	48	49	50
31	32	33	34	35	36	37	38	39	40
21	22	23	24	25	26	27	28	29	30
11	12	13	14	15	16	17	18	19	20
1	2	3	4	5	6	7	8	9	10

Modular Arithmetic and Congruence

CONGRUENCE

We say that two integers ***a*** and ***b*** are **congruent modulo *n*** if and only if ***n*|*(a-b)***, where ***n*** is a positive integer.
This is written as:

$$a \equiv b(mod\ n)$$

Example 1

Are 25 and 17 congruent modulo 4?

$$25 - 17 = 8. Since\ 4|8, \qquad 25 \equiv 17(mod\ 4)$$

Properties:

In the following, $a, b, c, d, k \in \boldsymbol{Z}$ *and* $n, m \in \boldsymbol{Z^+}$**:**

1. $a \equiv b(mod\ n) \Leftrightarrow \exists k \in Z\ such\ that\ a - b = kn$
2. $a \equiv b(mod\ n) \Leftrightarrow a\ and\ b\ have\ the\ same\ remainder\ (r \geq 0) when\ divided\ by\ n.$
3. $a \equiv a(mod\ n)$. This is known as the Reflexive Property
4. $a \equiv b(mod\ n) \Longrightarrow b \equiv a(mod\ n)$. This is known as the Symmetric Property
5. $a \equiv b(mod\ n)\ and\ b \equiv c(mod\ n) \Longrightarrow a \equiv c(mod\ n)$. This is known as the Transitive Property.
6. $a \equiv b(mod\ n) \Longrightarrow a + c \equiv b + c(mod\ n)\ and\ ac \equiv bc(mod\ n)$
7. $a \equiv b(mod\ n)\ and\ c \equiv d(mod\ n) \Longrightarrow a + c \equiv b + d(mod\ n)\ and\ ac \equiv bd(mod\ n)$
8. $a \equiv b(mod\ n) \Longrightarrow a^m \equiv b^m(mod\ n)$

Example 2

Prove congruence Property 5.

$$a \equiv b(mod\ n)\ and\ b \equiv c(mod\ n) \Longrightarrow a \equiv c(mod\ n)$$

$Since\ a \equiv b(mod\ n)\ and\ b \equiv c(mod\ n), then\ n|(a - b) and\ n|(b - c)$
From the division identity, we have:
$(a - b) = nq_1\ and\ (b - c) = nq_2\ \ where\ q_1, q_2 \in Z, remainders = 0$
$So\ (a - b) + (b - c) = nq_1 + nq_2$
$Thus\ a - c = n(q_1 + q_2) = nQ\ where\ q_1 + q_2 \in Z$
$Thus\ n|(a - c), so\ \ a \equiv c(mod\ n)$
Q.E.D.

The basic congruency properties can be regarded as rules for modular arithmetic, which operates with equality (=) replaced by congruence (≡). Properties 6 & 7 show that multiplication preserve congruency, but the operation is not reversible. This is obvious because division does not always give an integral answer. These properties allow some problems to be solved quite easily.

Example 3

Find the remainder when 3^{30} is divided by 7.
$3^3 = 27 \equiv -1(mod\ 7)$
$Thus\ 27^{10} \equiv (-1)^{10}(mod\ 7) \qquad Property\ 8$
$So\ 3^{30} \equiv 1(mod\ 7)$
From Property 2, the remainder when 3^{30} is divided by 7 is 1.

Exercises:

1. Prove Property 6
2. Prove Property 7.
3. Find the remainder when:
   i) 2^{30} is divided by 7
   ii) 5^{16} is divided by 24
   iii) 9^{120} is divided by 40
   iv) 2^{20} is divided by 41
   v) 23^{16} is divided by 7
4. Use the remainder when 3^{30} is divided by 7 to show that 3^{30}-1 is divisible by 7.
5. Show that $7|(3^{6n} - 1)\ \forall\ n \in Z^+$
6. Show that $24|(5^{2n} - 1)\ \forall\ n \in Z^+$
7. Show that $41|(2^{20n} - 1)\ \forall\ n \in Z^+$
8. Show that if $a \equiv b(mod\ n)$ and m|n, then $a \equiv b(mod\ m)$