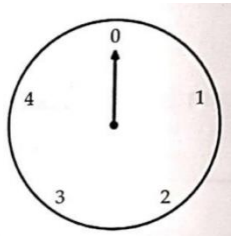
Euclidiad Introduction to Number Theory (Short Course)
Lecture 4 – Modular Arithmetic I

Today's topics: Modulus, Congruence, Residue, Addition and Subtraction in Modular Arithmetic

Example 1.
The clock below has only five numbers on its face: 0, 1, 2, 3 and 4. The clock has only one hand which moves around the circular face from 0 to 1 to 2 to 3 to 4 and back to 0 in that order. We set the clock to 0 ad let it begin ticking clockwise. The first 12 numbers it hits are 1, 2, 3, 4, 0, 1, 2, 3, 4, 0, 1 and 2.
(a) To what number does the clock point after 20 ticks?
(b) To what number does the clock point after 21 ticks?
(c) To what number does the clock point after 22 ticks?
(d) To what number does the clock point after 25 ticks?
(e) To what number does the clock point after 29 ticks?
(f) To what number does the clock point after 30 ticks?
(g) To what number does the clock point after 593 ticks?



In this example, we counted using only the 5 integers 0, 1, 2, 3, and 4. We call this system for counting modulo 5.

Modulus Definition

A modulus is a system for counting using only the fixed set of integers 0, 1, 2, …, $m-1$. When working in this modulus of m integers, we say that we are working with the integers modulo m.

Example 2.

Build a 10-row grid of integers according to the following rules:
(i) Place 4 integers in each row.
(ii) Let 0 be the leftmost integer in the top row.
(iii) For any pair of consecutive integers in a row, make the integer on the right 1 more than the integer on its left.
(iv) Make the first integer in each row after the first row 1 more than the last integer in the previous row.
Your first two rows should look like this:

0 1 2 3
4 5 6 7

(a) Which integers in the grid are in the same column as 0?
(b) Which integers in the grid are in the same column as 1?
(c) Which integers in the grid are in the same column as 2?
(d) Which integers in the grid are in the same column as 3?
(e) If you extend your grid to include a thousand rows, would the integer 3713 be in the same column as 0, 1, 2 or 3?

Congruence Definition

We say that two integers are congruent or equivalent modulo m when their difference is a multiple of m. Otherwise, they are incongruent in modulo m.

Two integers are congruent in a modulus when they share the same value. For instance, 3713 and 1 are congruent in modulo 4. From the counting grid in example 2, we see that 8 and 28 are congruent in modulo 4 and so are 17 and 33. We use the symbol " $\equiv$ " to express congruence and shorten "modulus" to "mod":

$$8 \equiv 28 \ (mod\ 4), 17 \equiv 33 \ (mod\ 4)$$

Since 25 and 38 do not share the same column, we see that they are incongruent in modulo 4. We write

$$25 \not\equiv 38 \ (mod\ 4), 12 \not\equiv 7 \ (mod\ 4)$$

For integers a and b, we say that $a \equiv b \ (mod\ m)$ if and only if $\frac{a-b}{m}$ is an integer.
Otherwise, $a \not\equiv b \ (mod\ m)$
(The difference between a and b is a multiple of m)

Example 3. Of the 100 smallest natural numbers, how many are congruent to each of the following?
(a) 0 (mod 7) (b) 1 (mod 7) (c) 2 (mod 7) (d) 3 (mod 7) (e) 4 (mod 7) (f) 5 (mod 7)
(f) 6 (mod 7)

For two integers, a and b, $a \equiv b \ (mod\ m)$ if and only if

$$a = q_1 m + r$$
$$b = q_2 m + r$$

where q_1, q_2 and r are integers and $0 \leq r < m$.

Example 4. Which of the following integers are congruent to 6 (mod 8)?
(a) -18 (b) 54 (c) 754 (d) 1036 (e) 13254

Example 5. Arrange the following integers in pairs that are congruent in modulo 12.

0	1	2	3	4	5	6	7	8	9	10	11
137	97	68	-97	177	-46	124	43	238	72	102	39

(Hint: Write each of those integers in the form $12n + r$ where n and r are integers and $0 \leq r < 12$.)

Residue Definition

We say that r is the modulo m residue of n when $n \equiv r \ (mod\ m)$ and $0 \leq r \leq n$.

Example 6. List all integers between -20 and 20 whose modulo 6 residues are 5.

Example 7. Note that $207 \equiv 25 \ (mod\ 7), 25 \equiv 4 \ (mod\ 7)$, and $207 \equiv 25 \ (mod\ 7)$. Is it always true that when $a \equiv b \ (mod\ 7)$ and $b \equiv c \ (mod\ 7)$, then $a \equiv c \ (mod\ 7)$?

If $a \equiv b \ (mod\ m), b \equiv c \ (mod\ m)$, then $a \equiv c \ (mod\ m)$

Example 8. Write each of the following integers in the form $8n + r$ where n and r are integers and $0 \leq r < 8$.

(a) 54 (b) 434 (c) 23 (d) 99 (e) 812

Example 9. Determine the residue of each of the following within the given modulus.

(a) 71 (mod 3) (b) -14 (mod 8) (c) 194 (mod 11) (d) -3944 (mod 9)

Example 10.

	Column 0	Column 1	Column 2	Column 3	Column 4	Column 5
	$6n$	$6n + 1$	$6n + 2$	$6n + 3$	$6n + 4$	$6n + 5$
$n = 0$	0	1	2	3	4	5
$n = 1$	6	7	8	9	10	11
$n = 2$	12	13	14	15	16	17
$n = 4$	18	19	20	21	22	23

Notice that $1 \equiv 7 \equiv 13 \equiv 19 \ (mod\ 6)$. Notice also that if we count up 1 from each of those integers, that the results are congruent modulo 6:

$$1 + 1 \equiv 7 + 1 \equiv 13 + 1 \equiv 19 + 1 \ (mod\ 6)$$

Let a_1 and a_2 be integers such that $a_1 \equiv a_2$.

(a) Show that $a_1 + 1 \equiv a_2 + 1 \ (mod\ 6)$

(b) Show that $a_1 - 1 \equiv a_2 - 1 \ (mod\ 6)$

(c) Show that $a_1 + b \equiv a_2 + b \ (mod\ 6)$ for any integer b.

Example 11. Let a_1, a_2, b_1, and b_2 be integers such that

$$a_1 \equiv a_2 \ (mod\ m)$$
$$b_1 \equiv b_2 \ (mod\ m)$$

Show that $a_1 + b_1 \equiv a_2 + b_2 \ (mod\ m)$.

If $a_1 \equiv a_2 \ (mod\ m), b_1 \equiv b_2 \ (mod\ m)$, then $a_1 + b_1 \equiv a_2 + b_2 \ (mod\ m)$.

Example 12. Note each of the following:

$$6004 = 1000 \times 6 + 4$$
$$603 = 100 \times 6 + 3$$
$$65 = 10 \times 6 + 5$$

Explain an easy way to quickly find the remainder when $6004 + 603 - 65 - 6$ is divided by 6.

Example 13. The remainders when two natural numbers are divided by 16 are 11 and 14 respectively.
(a) Find the remainder when their sum is divided by 16.
(b) Find the remainder when their sum is divided by 8.

Summary

- For integers a and b, we say that $a \equiv b \ (mod\ m)$ if and only if $\frac{a-b}{m}$ is an integer. Otherwise, $a \not\equiv b \ (mod\ m)$
- For two integers, a and b, $a \equiv b \ (mod\ m)$ if and only if
$$a = q_1 m + r$$
$$b = q_2 m + r$$
where q_1, q_2 and r are integers and $0 \leq r < m$.
- If $a \equiv b \ (mod\ m), b \equiv c \ (mod\ m)$, then $a \equiv c \ (mod\ m)$
- If $a_1 \equiv a_2 \ (mod\ m), b_1 \equiv b_2 \ (mod\ m),$ then $a_1 + b_1 \equiv a_2 + b_2 \ (mod\ m)$.

Lecture 4 - Homework Problems

Homework code : HW4
Issued on : 12th March 2022
Due date : 18th April 2022

Submit the solutions to at least 4 of the homework problems before due date. Problems 1 to 7 are each worth 5 points. Challenge problem is 10 points worth.

Problem 1. How many of the 200 smallest natural numbers are congruent to 1 (mod 9)? List all integers between -200 and 200 whose modulo 9 residues are 1.

Problem 2. Aung Aung Oo, Aung Aung Htoo and Aung Aung Tun are playing a game of marbles involving first arranging as many piles of 10 marbles as possible. Aung Aung Oo brought 239 marbles, Aung Aung Htoo brought 174 marbles and Aung Aung Tun brought 83 marbles. If all their marbles are grouped together, how many must be removed in order to start the game?

Problem 3. Prove that if $a \equiv b \ (mod\ m), b \equiv c \ (mod\ m)$, then $a \equiv c \ (mod\ m)$.

Problem 4. Which of the following statements of modular congruence are true and which are false?
(a) $118 \equiv 25 \ (mod\ 13)$ (b) $2701 \equiv 25 \ (mod\ 13)$ (c) $493 \equiv 873 \ (mod\ 10)$
(d) $2401 \equiv 147 \ (mod\ 49)$ (e) $183 \equiv 291 \ (mod\ 6)$

Problem 5. Determine the modulo 4 residue of the following sum:

$$1 + 2 + 3 + 4 + 5 + 6 + 7 + 8 + 9 + 10 + 11 + 12.$$

Problem 6. For how many positive integers N, is the remainder 6 when 111 is divided by N?

Problem 7. Suppose a and b are positive integers, neither of which is a multiple of 3. Find all possible remainders when $a^2 + b^2$ is divided by 3.

Challenge Problem

Problem 8. Ko Sai and Ko Thuta play a game with a pile of 82 toothpicks. The players take turns removing 1, 2, 3, or 4 toothpicks from the pile on each turn. The player that removes the last toothpick loses. Ko Sai goes first. Help him formulate a winning strategy.