Number Theory:

- Understand the concept of divisibility and the division algorithm.
- Understand how to use the Euclidean algorithm to find the greatest common divisor.
- Present an overview of the concepts of modular arithmetic.
- Discuss key concepts relating to prime numbers.
- Understand Fermat’s and Euler’s theorem.
- Understand theorem.
- Make a presentation on the topic of testing for primality.

Divisibility

- We say that a nonzero b **divides** a **if a = mb for some m, where a, b, and m are** integers.
- That is, b divides a if there is no remainder on division.
- The notation b|a is commonly used to mean b divides a.
- Also, if b|a, we say that b is a **divisor of a.**

Properties of Divisibility

- If $a|1$, then $a = \pm 1$.
- If $a|b$ and $b|a$, then $a = \pm b$.
- If $a \mid b$ and $b \mid c$, then $a \mid c$
  - e.g. $11 \mid 66$ and $66 \mid 198$ so $11 \mid 198$
- If $b|g$ and $b|h$, then $b|(mg + nh)$

  for arbitrary integers m and n

- If b|g,then g is of the form g=b x g1 for some integers g1.
- If b|h, then h is of the form h=b x h1 for some integers h1.
- So mg+nh=mbg1+nbh1=b x (mg1+nh1)
- Here b divides mg+nh

e.g. b = 7; g = 14; h = 63; m = 3; n = 2

7|14 and 7|63

To show 7|(3 x 14 +2 x 63),

we have(3 x 14+ 2 x 63)=7(3 x2 + 2 x 9) and

it is obvious that 7|(7(3 x2 + 2 x 9)).

hence 7 | 42+126 = 7|168

The Division Algorithm

- Given any positive integer n and any nonnegative integer a, if we divide a by n,
- we get an integer quotient q and an integer remainder r that obey the following relationship:

$$a = qn + r \quad \text{where } 0 <= r < n;\ q = \textbf{\textit{floor}}(a/n)$$

- The above equation is referred to as the division algorithm.
- **Example: 70 = (4 × 15) + 10**

Modular Arithmetic

- Given any positive integer n and any nonnegative integer a, if we divide a by n, we get an integer quotient q and an integer remainder r.
- In modular arithmetic we are only interested in the remainder (or residue) after division by some modulus.

The Modulus

- If *a is an integer and n is a positive integer, we define a mod n to be the remainder* when *a is divided by n. The integer n is called the* ***modulus.***

$$a = qn + r \qquad 0 \leq r < n; q = \lfloor a/n \rfloor$$

$$a = \lfloor a/n \rfloor \times n + (a \bmod n)$$

- 2 mod 12 = 2(remainder) , 40 mod 12 = 4(remainder)
- if negative number

  i.e -18 mod 14 =14 - (18 mod 14) =14 –(4) =10 (remainder)

congruent modulo N

- Two integers a and b are said to be congruent modulo n, if (a mod n) =(b mod n). This is written as
- a ≡b(mod n)

- *a* & *b* are **congruent** if: a mod n = b mod n
  - when divided by *n*, a & b have same remainder
  - eg. 100 mod 11 = 34 mod 11

    so 100 is congruent to 34

Modular Arithmetic Operations

- Z = Set of all integers = {…, -2, -1, 0, 1, 2, …}
- Z_n = Set of all non-negative integers less than n= {0, 1, 2, …, n-1}

  Ex: Z_2 = {0, 1}

  Z8 = { 0, 1, 2, 3, 4, 5, 6, 7}
- Addition, Subtraction, Multiplication, and division can all be defined in Zn
- We can perform arithmetic operations within the confines of this set Z_n , and this technique is known as **modular arithmetic.**

For Example:

- $(5+7) \bmod 8 = 4$
- $(4-5) \bmod 8 = 7$
- $(5*5) \bmod 8 = 1$

Modular arithmetic exhibits the properties.

- $[(a \bmod n) + (b \bmod n)] \bmod n = (a + b) \bmod n$
- $[(a \bmod n) - (b \bmod n)] \bmod n = (a - b) \bmod n$
- $[(a \bmod n) \times (b \bmod n)] \bmod n = (a \times b) \bmod n$

Here are examples of the three properties:

Given 11 mod 8 = 3;   15 mod 8 = 7

[(11 mod 8) + (15 mod 8)] mod 8 = 10 mod 8 = 2

(11 + 15) mod 8 = 26 mod 8 = 2

[(11 mod 8) – (15 mod 8)] mod 8 = –4 mod 8 = 4

(11 – 15) mod 8 = –4 mod 8 = 4

[(11 mod 8) x (15 mod 8)] mod 8 = 21 mod 8 = 5

(11 x 15) mod 8 = 165 mod 8 = 5

Modulo 8 Addition Example

+	0	1	2	3	4	5	6	7
0	0	1	2	3	4	5	6	7
1	1	2	3	4	5	6	7	0
2	2	3	4	5	6	7	0	1
3	3	4	5	6	7	0	1	2
4	4	5	6	7	0	1	2	3
5	5	6	7	0	1	2	3	4
6	6	7	0	1	2	3	4	5
7	7	0	1	2	3	4	5	6

Modulo 8 Multiplication

x	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

Modular Arithmetic Properties

Property	Expression
Commutative laws	$(w + x) \bmod n = (x + w) \bmod n$ $(w \times x) \bmod n = (x \times w) \bmod n$
Associative laws	$[(w + x) + y] \bmod n = [w + (x + y)] \bmod n$ $[(w \times x) \times y] \bmod n = [w \times (x \times y)] \bmod n$
Distributive law	$[w \times (x + y)] \bmod n = [(w \times x) + (w \times y)] \bmod n$
Identities	$(0 + w) \bmod n = w \bmod n$ $(1 \times w) \bmod n = w \bmod n$
Additive inverse $(-w)$	For each $w \in Z_n$, there exists a z such that $w + z \equiv 0 \bmod n$

Thank you