COT 3100C: INTRODUCTION TO DISCRETE STRUCTURES

SUMMER 2024

Number Theory

Part-1

Mesut Ozdag, Ph.D.
mesut.ozdag@ucf.edu

Section Summary

- Divisibility and Modular Arithmetic.
- Integer Representations and Algorithms.
- Primes and Greatest Common Divisors.
- Congruences.

Section:

Divisibility and Modular Arithmetic

Division

Definition: If a and b are integers with $a \neq 0$, then ***a divides b*** if there exists an integer c such that $\boldsymbol{b = ac}$.

- a is a ***factor*** or ***divisor*** of b,
- b is a ***multiple*** of a.
  - The notation $a \mid b$ denotes that a divides b.
  - If $a \mid b$, then b/a is an integer.
  - If a does not divide b, we write $a \nmid b$

Example: Determine whether $3 \mid 7$ and whether $3 \mid 12$.

Properties of Divisibility

Theorem 1: Let a, b, and c be integers, where $a \neq 0$.

i. If $a \mid b$ and $a \mid c$, then $a \mid (b + c)$;

ii. If $a \mid b$, then $a \mid bc$ for all integers c;

iii. If $a \mid b$ and $b \mid c$, then $a \mid c$.

Proof: (i) Suppose $a \mid b$ and $a \mid c$, then it follows that there are integers s and t with

$\boldsymbol{b = as}$ and $\boldsymbol{c = at}$.

$b + c = as + at = a(s + t)$.

$a \mid (b + c)$

Corollary: If a, b, and c be integers, where $a \neq 0$, such that $a \mid b$ and $a \mid c$, then $a \mid mb + nc$ whenever m and n are integers.

Division Theorem

Division Algorithm: If *a* is an integer and *d* a positive integer, then there are unique integers *q* and *r*, with $0 \leq r < d$, such that $a = dq + r$.

- *d* is called the *divisor*.
- *a* is called the *dividend*.
- *q* is called the *quotient*.
- *r* is called the *remainder*.

Definitions of Functions **div** and **mod**

$q = a \textbf{ div } d$

$r = a \textbf{ mod } d$

Examples:

- What are the quotient and remainder when 101 is divided by 11?
  - **Solution**: The quotient when 101 is divided by 11 is ➔ ***9 = 101 div 11,***
  - and the remainder is ➔ ***2 = 101 mod 11.***
- What are the quotient and remainder when −11 is divided by 3?
  - **Solution**: The quotient when −11 is divided by 3 is ➔ ***−4 = −11 div 3***,
  - and the remainder is ➔ ***1 = −11 mod 3***.

Congruence Relation

Definition: If a and b are integers and m is a positive integer, then

a* *is congruent to* *b* *modulo* *m if m divides $a - b$.

- The notation: $\boldsymbol{a \equiv b \pmod{m}}$
- $a \equiv b \pmod{m}$ is a ***congruence,*** and that m is its ***modulus***.
- Two integers are congruent mod m *iff* they have the same remainder when divided by m.
- If a is **not congruent** to b modulo m, $a \not\equiv b \pmod{m}$.

Example: Determine whether 17 is congruent to 5 modulo 6

and whether 24 and 14 are congruent to modulo 6.

Solution:

- $17 \equiv 5 \pmod{6}$ because 6 divides $17 - 5 = 12$.
- $24 \not\equiv 14 \pmod{6}$ since $24 - 14 = 10$ is not divisible by 6.

MESUT OZDAG, PH.D.
MESUT.OZDAG@UCF.EDU