CS1382 Discrete Computational Structures

Lecture 04: Number Theory

Spring 2019

Richard Matovu

TEXAS TECH UNIVERSITY

References

The materials of this presentation is mostly from the following:

- Discrete Mathematics and Its Applications (Text book and Slides)

  By Kenneth Rosen, 7th edition

Number Theory

- Study of the integers and their properties
  - Divisibility and the primality of integers.
  - Representations of integers, including binary and hexadecimal representations
  - Prime Numbers
  - Greatest common divisors and the Euclidean algorithm for computing them
- Applications
  - Generate pseudorandom numbers
  - Find check digits used to detect errors in various kinds of identification numbers
  - Assign memory locations to computer files
  - Cryptography
  - Computer and Internet Security

Definitions of Proofs

- A ***theorem*** is a statement that can be shown to be true using:
  - definitions
  - other theorems
  - axioms (statements which are given as true)
  - rules of inference
- A ***lemma*** is a “helping theorem” or a result which is needed to prove a theorem.
- A ***corollary*** is a result which follows directly from a theorem.
- A ***conjecture*** is a statement that is being proposed to be true. Once a proof of a conjecture is found, it becomes a theorem. It may turn out to be false.

CS1382 Discrete Computational Structures

Divisibility and Modular Arithmetic

Spring 2019

Richard Matovu

TEXAS TECH UNIVERSITY

Division

- If a and b are integers with $a \neq 0$, then ***a divides b*** if there exists an integer c such that $b = ac$.
  - When a divides b we say that a is a *factor* or *divisor* of b and that 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 $a \neq 0$.

1. If $a \mid b$ and $a \mid c$, then $a \mid (b + c)$;
2. If $a \mid b$, then $a \mid bc$ for all integers c;
3. If $a \mid b$ and $b \mid c$, then $a \mid c$.

Proof:

- Suppose $a \mid b$ and $a \mid c$, then it follows that there are integers s and t with $b = as$ and $c = at$.
- Hence, $b + c = as + at = a(s + t)$. Hence, $a \mid (b + c)$

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 Algorithm *(not really an algorithm)*

- When an integer is divided by a positive integer, there is a ***quotient*** and a ***remainder***.

  This is traditionally called the "Division Algorithm," but is really a theorem.

- **Division Algorithm:**

  If a is an integer and d is a positive integer, then there are unique integers q and r, with $0 \le r < d$, 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**

$q = a \textbf{ div } d$

$r = a \textbf{ mod } d$

Division Algorithm Examples

1. What are the quotient and remainder when 101 is divided by 11?

   - ***Solution:***

     The quotient when 101 is divided by 11 is $9 = 101 \text{ div } 11$, and the remainder is $2 = 101 \bmod 11$.

2. What are the quotient and remainder when -11 is divided by 3?

   - ***Solution:***

     The quotient when -11 is divided by 3 is $-4 = -11 \text{ div } 3$, and the remainder is $1 = -11 \bmod 3$.

Congruence Relation

- 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 **a ≡ b (mod m)** says that **a is congruent to b modulo m**.
  - We say that **a ≡ b (mod m)** is a ***congruence*** and that m is its ***modulus***.
  - Two integers are congruent mod m if and only if they have the same remainder when divided by m.
  - If a is not congruent to b modulo m, we write a $\not\equiv$ b (mod m)

Congruence Relation - Example

- Determine whether 17 is congruent to 5 modulo 6 and whether 24 and 14 are congruent 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.

More on Congruences

Theorem:

Let m be a positive integer. The integers a and b are congruent modulo m if and only if there is an integer k such that $a = b + km$.

- Proof:
  - If $a \equiv b \pmod{m}$, then (by the definition of congruence) $m \mid a - b$. Hence, there is an integer k such that $a - b = km$ and equivalently $a = b + km$.
  - Conversely, if there is an integer k such that $a = b + km$, then $km = a - b$. Hence, $m \mid a - b$ and $a \equiv b \pmod{m}$. ◀

The Relationship between (mod m) and **mod** m Notations

- The use of “mod” in $a \equiv b \pmod{m}$ and a **mod** $m = b$ are different.
  - $a \equiv b \pmod{m}$ is a relation on the set of integers.
  - In a **mod** $m = b$, the notation **mod** denotes a function.
- The relationship between these notations is made clear in this theorem.
- **Theorem:**

  Let a and b be integers, and let m be a positive integer.

  Then $a \equiv b \pmod{m}$ if and only if a **mod** $m = b$ **mod** m.

Congruences of Sums and Products

Theorem 5:

Let m be a positive integer. If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then

$a + c \equiv b + d \pmod{m}$ and $ac \equiv bd \pmod{m}$

Example:

Because $7 \equiv 2 \pmod{5}$ and $11 \equiv 1 \pmod{5}$, it follows from above theorem that

- $18 = 7 + 11 \equiv 2 + 1 = 3 \pmod{5}$
- $77 = 7 \cdot 11 \equiv 2 \cdot 1 = 2 \pmod{5}$

Algebraic Manipulation of Congruences

- Multiplying both sides of a valid congruence by an integer preserves validity.
  - If $a \equiv b \pmod{m}$ holds then $c \cdot a \equiv c \cdot b \pmod{m}$, where c is any integer
- Adding an integer to both sides of a valid congruence preserves validity.
  - If $a \equiv b \pmod{m}$ holds then $c + a \equiv c + b \pmod{m}$, where c is any integer
- Dividing a congruence by an integer does not always produce a valid congruence.
  - Example: The congruence $14 \equiv 8 \pmod{6}$ holds.

    But dividing both sides by 2 does not produce a valid congruence since $14/2 = 7$ and $8/2 = 4$, but $7 \not\equiv 4 \pmod{6}$.

Arithmetic Modulo m

Let $\boldsymbol{Z_m}$ be the set of nonnegative integers less than m: {0, 1, …., m−1}

- The operation $\mathbf{+_m}$ is defined as $a +_m b = (a + b) \bmod m$. This is ***addition modulo m***.
- The operation $\mathbf{\cdot_m}$ is defined as $a \cdot_m b = (a \cdot b) \bmod m$. This is ***multiplication modulo m***.
- Using these operations is said to be ***doing arithmetic modulo m***.

Example

- Find $7 +_{11} 9$ and $7 \cdot_{11} 9$.
  - $7 +_{11} 9 = (7 + 9) \bmod 11 = 16 \bmod 11 = 5$
  - $7 \cdot_{11} 9 = (7 \cdot 9) \bmod 11 = 63 \bmod 11 = 8$

Arithmetic Modulo m

- The operations $+_m$ and $\cdot_m$ satisfy many of the same properties as ordinary addition and multiplication.
  - **Closure:** If a and b belong to Z_m , then $a +_m b$ and $a \cdot_m b$ belong to Z_m .
  - **Associativity:** If a, b, and c belong to Z_m , then $(a +_m b) +_m c = a +_m (b +_m c)$ and $(a \cdot_m b) \cdot_m c = a \cdot_m (b \cdot_m c)$.
  - **Commutativity:** If a and b belong to Z_m , then $a +_m b = b +_m a$ and $a \cdot_m b = b \cdot_m a$.
  - **Identity elements:** The elements 0 and 1 are identity elements for addition and multiplication modulo m, respectively.
    - If a belongs to Z_m , then $a +_m 0 = a$ and $a \cdot_m 1 = a$.

continued →

Arithmetic Modulo m

- **Additive inverses:** If $a \neq 0$ belongs to Z_m , then $m - a$ is the additive inverse of a modulo m and 0 is its own additive inverse.
  - $a +_m (m - a) = 0$ and $0 +_m 0 = 0$
- **Distributivity:** If a, b, and c belong to Z_m , then
  - $a \cdot_m (b +_m c) = (a \cdot_m b) +_m (a \cdot_m c)$ and $(a +_m b) \cdot_m c = (a \cdot_m c) +_m (b \cdot_m c)$.

- ***Multiplicative inverses*** have not been included since they do not always exist.

  For example, there is no multiplicative inverse of 2 modulo 6.

Primitive Roots

A **primitive root** modulo a prime p is an integer r in $\mathbf{Z}_p$ such that every nonzero element of Z_p is a power of r.

Examples:

- Since every element of Z_{11} is a power of 2, 2 is a primitive root of 11.

  Powers of 2 modulo 11: $2^0 = 1$, $2^1 = 2$, $2^2 = 4$, $2^3 = 8$, $2^4 = 5$, $2^5 = 10$, $2^6 = 9$, $2^7 = 7$, $2^8 = 3$, $2^9 = 6$, $2^{10} = 0$.

- Since not all elements of Z_{11} are powers of 3, 3 is not a primitive root of 11.

  Powers of 3 modulo 11: $3^1 = 3$, $3^2 = 9$, $3^3 = 5$, $3^4 = 4$, $3^5 = 1$, and the pattern repeats for higher powers.

Important Fact: There is a primitive root modulo p for every prime number p.

Exercise

1. $-13 \bmod 2$
2. 17 mod 7
3. (417+93) mod 4
4. Is 5 a primitive root of 23?
5. Find a primitive root of 7?

Questions?

Thank You!