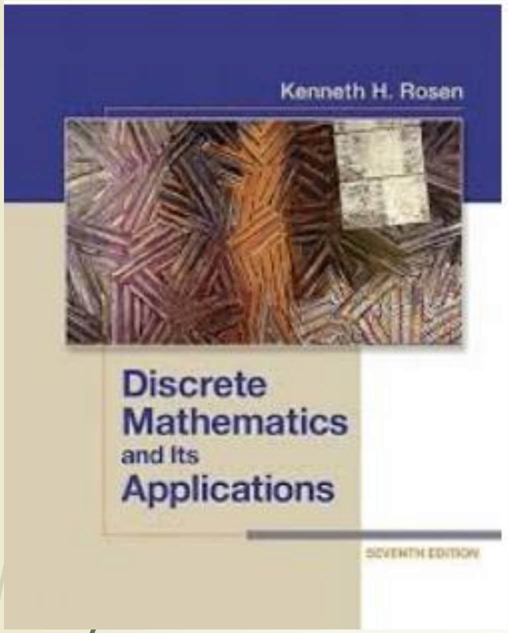
# MATH314 Advanced Discrete Mathematics

Dr. AbdulNaser Rashid

# About this Course

- Give mathematical background you need for computer science.
- Topics: Number Theory and Cryptography, Induction and Recursion, Advanced Counting Techniques, Boolean Algebra, Modeling Computation .
- These will come up again and again and again in higher-level CS courses.

# Textbook




- Textbook (optional): Discrete Mathematics and Its Applications by Kenneth Rosen.
- Textbook not a substitute for lectures:
  - Class presentation may not follow book
  - Skip many chapters and cover extra material

# Goals of a Course?

- A discrete mathematics course has more than one purpose:
  - Students should learn a particular set of mathematical facts and how to apply them;
  - More importantly, such a course should teach students how to think logically and mathematically.

# Requirements?

- Weekly written homework assignments,
- One midterm exams: in-class, closed-book,
- Scheduled for week 8,
- Final exam on week 16
- No make-up exams given unless you have serious, documented medical emergency.

# Grading?

- Final exam: 50% of final grade.
- Midterm: 30% of final grade
- Homework + QUIZES + Class Participations + Projects : 20% of final grade

# Number Theory and Cryptography

Chapter 4

With Question/Answer Animations

# Chapter Motivation

- *Number theory* is the part of mathematics devoted to the study of the integers and their properties.
- Key ideas in number theory include divisibility and the primality of integers.
- Representations of integers, including binary and hexadecimal representations, are part of number theory.
- Number theory has long been studied because of the beauty of its ideas, its accessibility, and its wealth of open questions.
- We'll use many ideas developed in Chapter 1 about proof methods and proof strategy in our exploration of number theory.
- Mathematicians have long considered number theory to be pure mathematics, but it has important applications to computer science and cryptography studied in Sections 4.5 and 4.6.

# Chapter Summary

- Divisibility and Modular Arithmetic
- Integer Representations and Algorithms
- Primes and Greatest Common Divisors
- Solving Congruences
- Applications of Congruences
- Cryptography

# Divisibility and Modular Arithmetic

Section 4.1

# Section Summary

- Division
- Division Algorithm
- Modular Arithmetic

# Division

- The ideas that we will develop in this section are based on the notion of divisibility.
- Division of an integer by a positive integer produces a quotient and a remainder. Working with these remainders leads to modular arithmetic, which plays an important role in mathematics and which is used throughout computer science.
- We will discuss some important applications of modular arithmetic later in this chapter, including generating pseudorandom numbers, assigning computer memory locations to files, constructing check digits, and encrypting messages.

# Division

**Definition**: 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 $a \neq 0$.

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 $b = as$ and $c = at$. Hence,

$$b + c = as + at = a(s + t). \quad \text{Hence, } a \mid (b + c)$$

(Exercises 3 and 4 ask for proofs of parts (ii) and (iii).)

**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.

Can you show how it follows easily from (ii) and (i) of Theorem 1?

# Division 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 $d$ a positive integer, then there are unique integers $q$ and $r$, with $0 \leq r < d$, such that

$$a = dq + r \text{ (proved in Section 5.2).}$$

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

# Division Algorithm

**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** $3$. *( Programming mod , %)*

# 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 $a \equiv b \pmod{m}$ says that *a* is congruent to *b* modulo *m*.
- We say that $a \equiv b \pmod{m}$ 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

$$a \not\equiv b \pmod{m}$$

**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.

# 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 3**: 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*. *(Proof in the exercises)*

# More on Congruences

- Theorem 4 provides a useful way to work with congruences.
- **Theorem 4**: 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 $a \equiv b \pmod{m}$.

# Congruences of Sums and Products

- Theorem 5 shows that additions and multiplications preserve congruences.
- **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 $ac \equiv bd \pmod{m}$

**Proof**:

- Because $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, by Theorem 4 there are integers $s$ and $t$ with $b = a + sm$ and $d = c + tm$. Therefore,

  $b + d = (a + sm) + (c + tm) = (a + c) + m(s + t)$ and

  $b\,d = (a + sm)\,(c + tm) = ac + m(at + cs + stm)$.
- Hence, $a+c \equiv b+d \pmod{m}$ and $ac \equiv bd \pmod{m}$.

# Congruences of Sums and Products

- **Example:**

  Because $7 \equiv 2 \pmod 5$ and $11 \equiv 1 \pmod 5$, it follows from Theorem 5 that:

  $$18 = 7 + 11 \equiv 2 + 1 = 3 \pmod 5$$

  $$77 = 7 \cdot 11 \equiv 2 \cdot 1 = 2 \pmod 5$$

- We must be careful working with congruences. Some properties we may expect to be true are not valid.
- **For Example:** 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, holds by Theorem 5 with $d = c$.

- 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, holds by Theorem 5 with $d = c$.

- Dividing a congruence by an integer does not always produce a valid congruence.

# Congruences of Sums and Products

- *But*, if ac ≡ bc (mod m), the congruence a ≡ b (mod m) may be false.
- *Similarly*, if a ≡ b (mod m) and c ≡ d (mod m), the congruence $a^c \equiv b^d$ (mod m) may be false.

  (See Exercise 37.)
- **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 $7 \not\equiv 4 \pmod{6}$.

See Section 4.3 for conditions when division is ok.

# Computing the **mod** *m* Function of Products and Sums

- We use the following corollary to Theorem 5, to show how to find the values of the **mod m** function at the sum and product of two integers using the values of this function at each of these integers.
- **Corollary**: Let $m$ be a positive integer and let $a$ and $b$ be integers. Then

$$(a + b)\ (\mathbf{mod}\ m) = ((a\ \mathbf{mod}\ m) + (b\ \mathbf{mod}\ m))\ \mathbf{mod}\ m$$

and

$$ab\ \mathbf{mod}\ m = ((a\ \mathbf{mod}\ m)\ (b\ \mathbf{mod}\ m))\ \mathbf{mod}\ m.$$

***(proof in text)***

# Arithmetic Modulo *m*

**Definitions**: Let $\mathbf{Z}_m$ be the set of nonnegative integers less than $m$: $\{0,1, \ldots., m-1\}$

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

**Example**: Find $7 +_{11} 9$ and $7 \cdot_{11} 9$?

**Solution**: Using the definitions above:

$$7 +_{11} 9 = (7 + 9) \ \mathbf{mod}\ 11 = 16\ \mathbf{mod}\ 11 = 5$$

$$7 \cdot_{11} 9 = (7 \cdot 9) \ \mathbf{mod}\ 11 = 63\ \mathbf{mod}\ 11 = 8$$

# 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 $\mathbf{Z}_m$ , then $a +_m b$ and $a \cdot_m b$ belong to $\mathbf{Z}_m$ .
  - ***Associativity***: If $a$, $b$, and $c$ belong to $\mathbf{Z}_m$ , 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 $\mathbf{Z}_m$ , then

    $$a +_m b = b +_m a \text{ and } a \cdot_m b = b \cdot_m a.$$
  - ***Identity elements***: The elements $0$ and $1$ are identity elements for addition and multiplication modulo $m$, respectively. If $a$ belongs to $\mathbf{Z}_m$ , then

    $$a +_m 0 = a \text{ and } a \cdot_m 1 = a.$$