4. Number Theory and Cryptography

Department of Mathematics & Statistics

ASU

1. **Divisibility and Modular Arithmetic**
2. **Integer Representation and Algorithms**
3. **Primes and Greatest Common Divisors**

- In this chapter, we will learn some of the important and fundamental concepts of number theory including many of those used in computer science.

- When we divide an integer by a positive integer, we can obtain a quotient and a remainder. When we work, in particular, with remainders, we are led to modular arithmetic which has some important applications of computer science.

Definitions

The notation $a \mid b$ denotes that $a \neq 0$ divides b, which means that $\exists q \in \mathbb{Z}$ such that $b = a\,q$. Then a is called a factor or divisor of b and b is called a multiple of a.

Example1

(1) Is $17 \mid 68$ true? (2) Is $17 \mid 84$ true?
(3) Is $17 \nmid 357$ true? (4) Is $17 \nmid 1001$ true?

Example2

1. Show that if $a \mid b$ and $b \mid a$ for $a, b \in \mathbb{Z}$, then $a = b$ or $a = -b$.
2. Find the quotient and remainder when (1) 19 is divided by 7? (2) 0 is divided by 19 (3) -1 is divided by 3.

The Division Algorithm

Let $b \in \mathbb{Z}$ and $a \in \mathbb{Z}^+$. Then $\exists! q \in Z$ and $\exists! r \in \mathbb{Z}$ with $0 \leq r < a$ such that $b = aq + r$.

Definitions

From the division algorithm, b is called the *dividend*, a is called the *divisor*, q is called the *quotient*, and r is called the *remainder*. The following notation is used to express the quotient and remainder:

$$q = b\ \mathbf{div} a, \quad r = b\ \mathbf{mod} a.$$

Definitions

Let $a, b \in \mathbb{Z}$ and $m \in \mathbb{Z}^+$. If $m \mid (a - b)$, then a is congruent to b modulo m and its notation is $a \equiv b (\text{mod } m)$. If a and b are not congruent modulo m, we use the notation $a \not\equiv b (\text{mod } m)$.

- **Different Notations**

1. $a \equiv b (\text{mod } m)$: represents a relation on the set of integers.
2. a **mod** $m = b$: represents a function

Theorem

Let $a, b \in \mathbb{Z}$ and $m \in \mathbb{Z}^+$.
*1. Then $a \equiv b (\text{mod } m) \Leftrightarrow a$ **mod** $m = b$ **mod** m.*
2. If $a \equiv b (\text{mod } m)$ and $c \equiv d (\text{mod } m)$,
then $a + c \equiv b + d (\text{mod } m)$ and $ac \equiv bd (\text{mod } m)$.

Theorem

Let $a, b \in \mathbb{Z}$ and $m \in \mathbb{Z}^+$. Then
*1. $(a+b)$ **mod** $m = ((a$ **mod** $m)+(b$ **mod** $m))$ **mod** m.*
*2. ab **mod** $m = ((a$ **mod** $m)(b$ **mod** $m))$ **mod** m.*

Example3

1 Suppose that $a, b \in \mathbb{Z}$, $a \equiv 4 \pmod{13}$, and $a \equiv 9 \pmod{13}$. Find integer c with $0 \leq c \leq 12$) such that
(1) $c \equiv 9a \pmod{13}$ (2) $c \equiv a+b \pmod{13}$
(3) $c \equiv 2a+3b \pmod{13}$ (4) $c = a^2+b^2 \pmod{13}$
2. Evaluate the following ones:(1) 13 **mod** 3 (2) -221 **mod** 23
3. Find the integer a such that
(1) $a \equiv -15 \pmod{27}$ and $-22 \leq a \leq 0$
(2) $a \equiv 24 \pmod{31}$ and $90 \leq a \leq 110$
4. Decide whether the followings are congruent to 3 modulo 7
(1) 80 (2) 103 (3) -29 (4) -122
5 (1) (-133 **mod** 23+ 261 **mod** 23) **mod** 23.
(2) (457 **mod** $23 \cdot 182$ **mod** 23) **mod** 23.