Number Theory and Cryptography

Chapter 4

With Question/Answer Animations

Chapter Overview

- *Number theory* is the study of **integers** & their properties.
- Key ideas include **divisibility** and **primality**.
- Representations of integers, including **binary** and **hexadecimal**, may be considered part of number theory.
- Due to its beauty, accessibility, and wealth of open questions, number theory has attracted many mathematicians.
- In our exploration of number theory, we'll develop many of the proof methods and strategies introduced in chapter 1.
- Mathematicians consider number theory to be **pure** mathematics, but it has important **applications** to computer science and cryptography (Sections 4.5 and 4.6).

Chapter Summary

4.1 **Divisibility and Modular Arithmetic**

4.2 Integer Representations and Algorithms

4.3 Primes and Greatest Common Divisors

4.4 Solving Congruences

4.5 Applications of Congruences

4.6 Cryptography

Divisibility and Modular Arithmetic

Section 4.1

Section Summary

- Division
- Division Algorithm
- Modular Arithmetic

Definition of Divisibility

If a and b are integers with $a \neq 0$, then *a divides b* if $\exists c \in Z$ such that $b = ac$, i.e., if $b/a \in Z$.

- 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 does not divide b, we write $a \nmid b$.

Exercise: Determine if $3 \mid 7$ and if $3 \mid 12$.

$3 \nmid 7$ ($7/3$ is not an integer)

but $3 \mid 12$ ($12/3 = 4$)

Properties of Divisibility

Theorem 1: Let $a \neq 0$, b, $c \in Z$.

i. If $a \mid b$ and $a \mid c$, then $a \mid (b + c)$;
ii. If $a \mid b$, then $a \mid bc$ $\forall c \in Z$;
iii. If $a \mid b$ and $b \mid c$, then $a \mid c$.

Proof: (i) If $a \mid b$ and $a \mid c$, then $\exists s, t \in Z$ with $b = as$ and $c = at$. Hence,

$$b + c = as + at = a(s + t). \quad \therefore a \mid (b + c).$$

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

Corollary: If $a \neq 0$, b, $c \in Z$, such that $a \mid b$ and $a \mid c$, then

$$a \mid mb + nc \text{ if } m, n \in Z.$$

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 "Division Algorithm," is really a theorem.

Division Algorithm: If $a \in Z$ & $d \in Z^+$, then $\exists! q\ r$, with $0 \le r < d$, such that $a = d\ q + r$ (*proved in Section* 5.2).

dividend	divisor	quotient	remainder

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

$q = a$ **div** d
$r = a$ **mod** d

Examples:

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

Definition of Congruence Relation

If $a, b \in Z$, $m \in Z^+$, then a is *congruent* to b *modulo* m if $m \mid a - b$. (m is its *modulus*)

- We write $a \equiv b \pmod{m}$
- 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 if $17 \equiv 5 \pmod{6}$ & if $24 \equiv 14 \pmod{6}$

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 4: Let $a, b \in Z$, $m \in Z^+$ $a \equiv b \pmod{m}$ if and only if $\exists k \in Z$ such that $a = b + km$.

Proof:

$a \equiv b \pmod{m}$

iff $m \mid a - b$

iff $\exists k \in Z$ such that $a - b = km$

iff $\exists k \in Z$ such that $a = b + km$ ◀

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

- "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 by:

Theorem 3: Let $a, b \in Z$, $m \in Z^+$. Then $a \equiv b \pmod{m}$ iff

$$a \mathbf{\ mod\ } m = b \mathbf{\ mod\ } m.$$

(*Proof in the exercises*)

Congruences of Sums and Products

Theorem 5: If $a, b, c, d \in Z$, $m \in Z^+$, $a \equiv b$, $c \equiv d \pmod{m}$, then $a + c \equiv b + d \pmod{m}$ and $ac \equiv bd \pmod{m}$

Proof: Because $a \equiv b$, $c \equiv d \pmod{m}$, by Theorem 4

$\exists s, t$ with $b = a + sm$ and $d = c + tm$. So

- $b + d = (a + sm) + (c + tm) = (a + c) + m(s + t)$ and
- $b\,d = (a + sm)\,(c + tm) = ac + m(at + cs + stm)$.

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

Example: Because $7 \equiv 2 \pmod{5}$ and $11 \equiv 1 \pmod{5}$,

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

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

Algebraic Manipulation of Congruences

- Multiplying or adding to both sides preserves validity:

  If $a \equiv b \pmod{m}$ holds and $c \in Z$ then

  $$c \cdot a \equiv c \cdot b \pmod{m} \text{ and } c + a \equiv c + b \pmod{m}$$

  hold by Theorem 5 with $d = c$.

- Dividing 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 $7 \not\equiv 4 \pmod{6}$.

See Section 4.3 for conditions when division is ok.

Computing **mod** *m* for · and +

Use the following to compute the remainder of product or sum when divided by m:

Corollary: If $a, b \in Z$, $m \in Z^+$, then

$(a + b)$ (**mod** m) = $((a$ **mod** $m) + (b$ **mod** $m))$ **mod** m

and

ab **mod** m = $((a$ **mod** $m)$ $(b$ **mod** $m))$ **mod** m.

(*proof in text*)

Definitions: Arithmetic Modulo *m*

Let $\mathbf{Z}_m$ be the set of nonnegative integers less than m:

$$\{0,1, \ldots., m-1\}$$

- *addition modulo m* $+_m$ is $a +_m b = (a + b)$ **mod** m.
- *multiplication modulo m* $\cdot_m$ is $a \cdot_m b = (a \cdot b)$ **mod** m.

Using these operations is doing *arithmetic modulo m*.

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

Solution: Using the definitions above:

- $7 +_{11} 9 = (7 + 9)$ **mod** $11 = 16$ **mod** $11 = 5$
- $7 \cdot_{11} 9 = (7 \cdot 9)$ **mod** $11 = 63$ **mod** $11 = 8$

Arithmetic Modulo *m*

$+_m$ and $\cdot_m$ satisfy many of same props as ordinary + and $\cdot$.

- *Closure*: If $a, b \in \mathbf{Z}_m$, then $a +_m b \in \mathbf{Z}_m$ and $a \cdot_m b \in \mathbf{Z}_m$ as well.
- *Associativity*: If $a, b, c \in \mathbf{Z}_m$, 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 $a, b \in \mathbf{Z}_m$, then

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

- *Identity*: 0 and 1 are identity elements for + and * mod *m*:
  - If $a \in \mathbf{Z}_m$, then $a +_m 0 = a$ and $a \cdot_m 1 = a$.
- $a \neq 0 \in \mathbf{Z}_m \Rightarrow m - a$ is the *additive inverse* of a mod m.
  - $a +_m (m - a) = 0$ and $0 +_m 0 = 0$ (0 is its own add inv.)
- *Distributivity*: If a, b, and c belong to $\mathbf{Z}_m$, then
  - $a \cdot_m (b +_m c) = (a \cdot_m b) +_m (a \cdot_m c)$
  - $(a +_m b) \cdot_m c = (a \cdot_m c) +_m (b \cdot_m c)$

Arithmetic Modulo *m* (cont.)

- Exercises 42-44 ask for proofs of these properties.
- Multiplicative inverses have not been included since they do not always exist.
  - For example, there is no multiplicative inverse of 2 mod 6.
  - Existence of an inverse is closely tied to existence of division already mentioned, as we will see in section 4.4.