Discrete Structures for Computer Science

William Garrison
bill@cs.pitt.edu
6311 Sennott Square

Lecture #20: Divisibility and Modular Arithmetic

University of Pittsburgh

Today's Topics

Integers and division

- Divisibility
- The division algorithm
- Modular arithmetic

What is number theory?

Number theory is the branch of mathematics that explores the integers and their properties.

Number theory has many applications within computer science, including:

- Organizing data
- Encrypting sensitive data
- Developing error correcting codes
- Generating "random" numbers
- …

We will only scratch the surface…

The notion of divisibility is one of the most basic properties of the integers

Definition: If a and b are integers and $a \neq 0$, we say that a divides b iff there is an integer c such that $b = ac$. We write $a \mid b$ to say that a divides b, and $a \nmid b$ to say that a does not divide b.

Mathematically: $a \mid b \leftrightarrow \exists c \in \mathbf{Z}\ (b = ac)$

Note: If $a \mid b$, then

- a is called a factor of b
- b is called a multiple of a

We've been using the notion of divisibility all along!

- $E = \{x \mid x = 2k \wedge k \in \mathbf{Z}\}$

Division examples

Examples:

- Does $4 \mid 16$?
- Does $3 \mid 11$?
- Does $7 \mid 42$?

Question: Let n and d be two positive integers. How many positive integers not exceeding n are divisible by d?

Answer: We want to count the number of integers of the form dk that are no more than n. That is, we want to know the number of integers k with $0 < dk \leq n$, or $0 < k \leq n/d$. Therefore, there are $\lfloor n/d \rfloor$ positive integers not exceeding n that are divisible by d.

Important properties of divisibility

Property 1: If $a \mid b$ and $a \mid c$, then $a \mid (b + c)$

Property 2: If $a \mid b$, then $a \mid bc$ for any integer c.

Property 3: If $a \mid b$ and $b \mid c$, then $a \mid c$.

Division algorithm

Theorem: Let a be an integer and let d be a positive integer. There are unique integers q and r, with $0 \leq r < d$, such that $a = dq + r$.

For historical reasons, the above theorem is called the division algorithm, even though it isn't an algorithm!

Terminology: Given $a = dq + r$

- a is called the dividend
- d is called the divisor
- q is called the quotient
- r is called the remainder
- $q = a \ \mathbf{div} \ d$
- $r = a \ \mathbf{mod} \ d$

div and mod are operators

Examples

Question: What are the quotient and remainder when 123 is divided by 23?

Answer: We have that $123 = 23 \times 5 + 8$. So the quotient is $123 \textbf{ div } 23 = 5$, and the remainder is $123 \textbf{ mod } 23 = 8$.

Question: What are the quotient and remainder when -11 is divided by 3?

Answer: Since $-11 = 3 \times -4 + 1$, we have that the quotient is -4 and the remainder is 1.

Recall that since the remainder must be non-negative, $3 \times -3 - 2$ is not a valid use of the division theorem!

In-class exercises

Problems 1-4: On Top Hat

Sometimes, we care only about the remainder of an integer after it is divided by some other integer

Example: What time will it be 22 hours from now?

Answer: If it is 11 am now, it will be $(11 + 22)\ \mathbf{mod}\ 24 = 33\ \mathbf{mod}\ 24 = 9$ am in 22 hours.

Since remainders can be so important, they have their own special notation!

Definition: If a and b are integers and m is a positive integer, we say that a is congruent to b modulo m iff $m \mid (a - b)$. We write this as $a \equiv b \pmod{m}$.

Note: $a \equiv b \pmod{m}$ iff $a \ \mathbf{mod}\ m = b \ \mathbf{mod}\ m$.

Examples:

- Is 17 congruent to 5 modulo 6?
- Is 24 congruent to 14 modulo 6?

Properties of congruencies

Theorem: Let m be a positive integer. The integers a and b are congruent modulo m ($a \equiv b \pmod{m}$) iff there is an integer k such that $a = b + km$.

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

- $(a + c) \equiv (b + d) \pmod{m}$
- $ac \equiv bd \pmod{m}$

These properties mean we can use addition and multiplication as usual, even if we are only considering remainders (mod m)

Proving one of these congruence rules

WTP: If m is a positive integer, $a \equiv b \pmod{m}$, and $c \equiv d \pmod{m}$, then $(a + c) \equiv (b + d) \pmod{m}$

Assume $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$

- So $m \mid (a - b)$ and $m \mid (c - d)$
- This means $a - b = km$ and $c - d = jm$, for some integers k and j

Consider $(a + c) - (b + d) = (a - b) + (c - d) = km + jm = m(j + k)$

- Thus, $m \mid \big((a + c) - (b + d)\big)$
- This means $(a + c) \equiv (b + d) \pmod{m}$. $\square$

Defining arithmetic restricted to remainders when dividing by m

$\mathbf{Z}_m$ denotes the set of nonnegative integers less than m

- i.e., the remainders when dividing by m

From our previous theorem we can show that **mod** "preserves" addition and multiplication

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

Thus, we can define versions of addition and multiplication that are restricted to this set

- $a +_m b = (a + b) \mathbf{\ mod\ } m$
- $a \cdot_m b = (a \cdot b) \mathbf{\ mod\ } m$

These operations form arithmetic modulo m

Examples

Use the definition of addition and multiplication in $\mathbf{Z}_m$ to evaluate each of the following.

$6 +_{12} 10$

- $6 +_{12} 10 = (6 + 10)$ **mod** 12
- $= 16$ **mod** $12 = 4$

$6 \cdot_{12} 10$

- $6 \cdot_{12} 10 = (6 \cdot 10)$ **mod** 12
- $= 60$ **mod** $12 = 0$

$15 \cdot_{12} 22$

- $15 \cdot_{12} 22 = (15 \cdot 22)$ **mod** 12
- $= (3 \cdot 10)$ **mod** 12
- $= 30$ **mod** $12 = 6$

In-class exercises

Problem 5-6: On Top Hat

Final thoughts

- Number theory is the study of integers and their properties
- Divisibility, modular arithmetic, and congruency are important topics
  - Later in Chapter 4 we will see how these are used throughout computer science
- Next time:
  - Integer representations (Section 4.2)