CS 441 Discrete Mathematics for CS
Lecture 12

Integers and division

Milos Hauskrecht
milos@cs.pitt.edu
5329 Sennott Square

Matrix transpose

Definition:

- Let $\mathbf{A} = [a_{ij}]$ be an m x n matrix. The **transpose** of **A**, denoted by $\mathbf{A}^T$,is the n x m matrix obtained by interchanging the rows and columns of **A**.

If $\mathbf{A}^T = [b_{ij}]$, then $b_{ij} = a_{ji}$ for $i = 1,2,\ldots,n$ and $j = 1,2, \ldots,m$.

The transpose of the matrix $\begin{bmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{bmatrix}$ is the matrix $\begin{bmatrix} 1 & 4 \\ 2 & 5 \\ 3 & 6 \end{bmatrix}$.

Symmetric matrix

Definition:

- A square matrix **A** is called **symmetric** if $\mathbf{A} = \mathbf{A}^T$.
- Thus $\mathbf{A} = [a_{ij}]$ is symmetric if $a_{ij} = a_{ji}$ for i and j with $1 \leq i \leq n$ and $1 \leq j \leq n$.

- **Example:**

1	1	0	0
1	0	1	0
0	1	1	1
0	0	1	0

- Is it a symmetric matrix?

Symmetric matrix

Definition:

- A square matrix **A** is called **symmetric** if $\mathbf{A} = \mathbf{A}^T$.
- Thus $\mathbf{A} = [a_{ij}]$ is symmetric if $a_{ij} = a_{ji}$ for i and j with $1 \leq i \leq n$ and $1 \leq j \leq n$.

- **Example:**

1	1	0	0
1	0	1	0
0	1	1	1
0	0	1	0

- Is it a symmetric matrix? yes

Zero-one matrix

Definition:

- A matrix all of whose entries are either 0 or 1 is called **a zero-one matrix.**

- Algorithms operating on discrete structures represented by zero-one matrices are based on Boolean arithmetic defined by the following Boolean operations:

$$b_1 \wedge b_2 = \begin{cases} 1 & \text{if } b_1 = b_2 = 1 \\ 0 & \text{otherwise} \end{cases}$$

$$b_1 \vee b_2 = \begin{cases} 1 & \text{if } b_1 = 1 \text{ or } b_2 = 1 \\ 0 & \text{otherwise} \end{cases}$$

Join and meet of matrices

Definition: Let A and B be two matrices:

$$\mathbf{A} = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix}, \qquad \mathbf{B} = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 1 & 0 \end{bmatrix}.$$

- **The join of A and B is:**

$$\mathbf{A} \vee \mathbf{B} = \begin{bmatrix} 1 \vee 0 & 0 \vee 1 & 1 \vee 0 \\ 0 \vee 1 & 1 \vee 1 & 0 \vee 0 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 0 \end{bmatrix}.$$

- **The meet of A and B is**

$$\mathbf{A} \wedge \mathbf{B} = \begin{bmatrix} 1 \wedge 0 & 0 \wedge 1 & 1 \wedge 0 \\ 0 \wedge 1 & 1 \wedge 1 & 0 \wedge 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}.$$

CS 441 Discrete Mathematics for CS
Lecture 12

Integers and division

Milos Hauskrecht
milos@cs.pitt.edu
5329 Sennott Square

Integers and division

- **Number theory** is a branch of mathematics that explores integers and their properties.
- **Integers:**
  - **Z   integers {…, -2,-1, 0, 1, 2, …}**
  - **Z^+ positive integers {1, 2, …}**

- Number theory has many applications within computer science, including:
  - Storage and organization of data
  - Encryption
  - Error correcting codes
  - Random numbers generators

Division

Definition: Assume 2 integers a and b, such that a =/ 0 (a is not equal 0). We say that **a divides b** if there is an integer c such that b = ac. When a divides b we say that **a is a *factor* of b** and that **b is *multiple* of a**.

- The fact that a divides b is denoted as **a | b.**

Examples:

- 4 | 24 True or False ? **True**
  - 4 is a factor of 24
  - 24 is a multiple of 4
- 3 | 7 True or False ?

CS 441 Discrete mathematics for CS M. Hauskrecht

Division

Definition: Assume 2 integers a and b, such that a =/ 0 (a is not equal 0). We say that **a divides b** if there is an integer c such that b = ac. If a divides b we say that **a is a *factor* of b** and that **b is *multiple* of a**.

- The fact that a divides b is denoted as **a | b.**

Examples:

- 4 | 24 True or False ? **True**
  - 4 is a factor of 24
  - 24 is a multiple of 4
- 3 | 7 True or False ? **False**

CS 441 Discrete mathematics for CS M. Hauskrecht

Divisibility

All integers divisible by d>0 can be enumerated as:

– *.., -kd, …, -2d, -d, 0, d, 2d, …, kd, …*

- **Question:**

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

- **Answer:**

  Count the number of integers *kd* that are less than *n.* What is the the number of integers *k* such that $0 < kd \leq n$?

  $0 < kd \leq n \rightarrow 0 < k \leq n/d$. Therefore, there are $\lfloor n/d \rfloor$ positive integers not exceeding *n* that are divisible by d.

Divisibility

Properties:

- Let a, b, c be integers. Then the following hold:
  1. if a | b and a | c then a | (b +c)
  2. if a | b then a | bc for all integers c
  3. if a | b and b | c then a | c

Proof of 1: if a | b and a | c then a | (b +c)

- from the definition of divisibility we get:
- b=au and c=av where u,v are two integers. Then
- (b+c) = au +av = a(u+v)
- **Thus a divides b+c.**

Divisibility

Properties:

- Let a, b, c be integers. Then the following hold:
  1. if a | b and a | c then a | (b +c)
  2. if a | b then a | bc for all integers c
  3. if a | b and b | c then a | c

Proof of 2: if a | b then a | bc for all integers c

- If a | b, then there is some integer u such that b = au.
- Multiplying both sides by c gives us bc = auc, so by definition, a | bc.
- **Thus a divides bc.**

Primes

Definition: A positive integer p that greater than 1 and that is divisible only by 1 and by itself (p) is called **a prime**.

Examples: 2, 3, 5, 7, …

1 | 2 and 2 | 2, 1 |3 and 3 | 3, etc

Primes

Definition: A positive integer p that greater than 1 and that is divisible only by 1 and by itself (p) is called **a prime**.

Examples: 2, 3, 5, 7, …

1 | 2 and 2 | 2,   1 |3 and 3 | 3, etc

What is the next prime after 7?

- ?

Primes

Definition: A positive integer p that greater than 1 and that is divisible only by 1 and by itself (p) is called **a prime**.

Examples: 2, 3, 5, 7, …

1 | 2 and 2 | 2,   1 |3 and 3 | 3, etc

What is the next prime after 7?

- 11

Next?

Primes

Definition: A positive integer p that greater than 1 and that is divisible only by 1 and by itself (p) is called **a prime**.

Examples: 2, 3, 5, 7, …

1 | 2 and 2 | 2, 1 |3 and 3 | 3, etc

What is the next prime after 7?

- 11

Next?

- 13

Primes

Definition: A positive integer that is greater than 1 and is not a prime is called **a composite.**

Examples: 4, 6, 8, 9, …

Why?

2 | 4

3 | 6 or 2 | 6

2 | 8 or 4 | 8

3 | 9

The Fundamental theorem of Arithmetic

Fundamental theorem of Arithmetic:

- Any positive integer greater than 1 can be expressed as a product of prime numbers.

Examples:

- 12 = 2*2*3
- 21 = ?

The Fundamental theorem of Arithmetic

Fundamental theorem of Arithmetic:

- Any positive integer greater than 1 can be expressed as a product of prime numbers.

Examples:

- 12 = 2*2*3
- 21 = 3*7

- Process of finding out factors of the product: **factorization**.

Primes and composites

Factorization of composites to primes:

- $100 = 2*2*5*5 = 2^2*5^2$
- $99 = 3*3*11 = 3^2*11$

Important question:

- How to determine whether the number is a prime or a composite?

Primes and composites

- How to determine whether the number is a prime or a composite?

Simple approach (1):

- Let n be a number. To determine whether it is a prime we can test if any number $x < n$ divides it. If yes it is a composite. If we test all numbers $x < n$ and do not find the proper divisor then n is a prime.

Primes and composites

- How to determine whether the number is a prime or a composite?

Simple approach (1):

- Let n be a number. To determine whether it is a prime we can test if any number $x < n$ divides it. If yes it is a composite. If we test all numbers $x < n$ and do not find the proper divisor then n is a prime.
- Is this the best we can do?
- **No.** The problem here is that we try to test all the numbers. But this is not necessary.
- **Idea:** Every composite factorizes to a product of primes. So it is sufficient to test only the primes $x < n$ to determine the primality of n.

Primes and composites

- How to determine whether the number is a prime or a composite?

Approach 2:

- Let n be a number. To determine whether it is a prime we can test if any prime number x < n divides it. If yes it is a composite. If we test all primes $x < n$ and do not find a proper divisor then n is a prime.

Primes and composites

- How to determine whether the number is a prime or a composite?

Approach 2:

- Let *n* be a number. To determine whether it is a prime we can test if any prime number x < n divides it. If yes it is a composite. If we test all primes $x < n$ and do not find the proper divisor then *n* is a prime.
- If *n* is relatively small the test is good because we can enumerate (memorize) all small primes
- But if *n* is large there can be larger not obvious primes

Primes and composites

- How to determine whether the number is a prime or a composite?

Approach 2:

- Let *n* be a number. To determine whether it is a prime we can test if any prime number x < n divides it. If yes it is a composite. If we test all primes $x < n$ and do not find the proper divisor then *n* is a prime.
- If *n* is relatively small the test is good because we can enumerate (memorize) all small primes
- But if *n* is large there can be larger not obvious primes

Example: Is 91 a prime number?

- Easy primes 2,3,5,7,11,13,17,19 ..
- But how many primes are there that are smaller than 91

Primes and composites

Theorem: If n is a composite then *n* has a prime divisor less than or equal to $\sqrt{n}$.

Proof:

- If n is composite, then it has a positive integer factor *a* such that $1 < a < n$ by definition. This means that $n = ab$, where *b* is an integer greater than 1.
- Assume $a > \sqrt{n}$ and $b > \sqrt{n}$. Then $ab > \sqrt{n}\sqrt{n} = n$, which is a contradiction. So either $a \leq \sqrt{n}$ *or* $b \leq \sqrt{n}$.
- Thus, *n* has a divisor less than $\sqrt{n}$.
- By the fundamental theorem of arithmetic, this divisor is either prime, or is a product of primes. In either case, *n* has a prime divisor less than $\sqrt{n}$.

Primes and composites

Theorem: If n is a composite then n has a prime divisor less than or equal to $\sqrt{n}$.

Approach 3:

- Let *n* be a number. To determine whether it is a prime we can test if any prime number $x < \sqrt{n}$ divides it.

Example 1: Is 101 a prime?

- Primes smaller than $\sqrt{101}$ = 10.xxx are: 2,3,5,7
- 101 is not divisible by any of them
- **Thus 101 is a prime**

Primes and composites

Theorem: If n is a composite that n has a prime divisor less than or equal to $\sqrt{n}$.

Approach 3:

- Let n be a number. To determine whether it is a prime we can test if any prime number x < $\sqrt{n}$ divides it.

Example 1: Is 101 a prime?

- Primes smaller than $\sqrt{101}$ = 10.xxx are: 2,3,5,7
- 101 is not divisible by any of them
- **Thus 101 is a prime**

Example 2: Is 91 a prime?

- Primes smaller than $\sqrt{91}$ are: 2,3,5,7
- 91 is divisible by 7
- **Thus 91 is a composite**

Primes

Question: How many primes are there?

Theorem: There are infinitely many primes.

Proof by Euclid.

- Proof by contradiction:
  - Assume there is a finite number of primes: $p_1,p_2, \ldots p_n$
- Let $Q = p_1p_2\ldots p_n + 1$ be a number.
- None of the numbers $p_1,p_2, \ldots, p_n$ divides the number Q.
- This is a contradiction since we assumed that we have listed all primes.

Division

Let a be an integer and d a positive integer. Then there are unique integers, q and r, with 0 <= r < d, such that

a = dq + r.

Definitions:

- a is called the **dividend**,
- d is called the **divisor**,
- q is called the **quotient** and
- r the **remainder** of the division.

Relations:

- **q = a div d , r = a mod d**