CS 441 Discrete Mathematics for CS
Lecture 14

Integers and division

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

Integers and division

- **Integers:**
  - **Z integers {…, -2,-1, 0, 1, 2, …}**
  - **Z^+ positive integers {1, 2, …}**
- Part of discrete math that concerns integers and their properties are studied within the **number theory**
- Here, in this course we study the property of divisibility.

Primes

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

Examples: 2, 3, 5, 7, 11, …

Why are primes important?

Fundamental theorem of Arithmetic:

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

Examples:

- 12 =

Primes

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

Examples: 2, 3, 5, 7, 11, …

Why are primes important?

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 =

Primes

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

Examples: 2, 3, 5, 7, 11, …

Why are primes important?

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**.

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 ?

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 ?

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 ? **False**

Divisibility

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

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

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)

Divisibility

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

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

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.**

Primes and composites

Definition: A positive integer p greater than 1 is called ***a prime***, if the only positive factors of p are 1 and p. A positive integer that is greater than 1 and is not a prime is called ***a composite***.

Factorization of composites to primes:

- 100 = 2*2*5*5 = $2^2 * 5^2$
- 99 = …

Primes and composites

Definition: A positive integer p greater than 1 is called ***a prime***, if the only positive factors of p are 1 and p. A positive integer that is greater than 1 and is not a prime is called ***a composite***.

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?

A simple approach:

- 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 a proper divisor then n is a prime.

Primes and composites

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

A simple approach:

- 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?

Primes and composites

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

A 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.
- 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 the 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 97

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 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 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**

Example 2: Is 91 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 $\sqrt{97}$ 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.

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 $Q = p_1 p_2 \ldots p_n + 1$ 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**