CS 441 Discrete Mathematics for CS
Lecture 11

Integers and division

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

Integers and division

- **Number theory** is the branch of mathematics that explores the 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 ?

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. 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**

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 $0 \leq kd \leq n$?

  $0 \leq kd \leq n$ → $0 \leq k \leq n/d$. 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)

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

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 = ?

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

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 = …

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?

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.

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?

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.
- **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 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 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 $a \le \sqrt{n}$ *or* $b \le \sqrt{n}$.
- 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 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 $\sqrt{91}$ are: 2,3,5,7
- ?

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.

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

$$\mathbf{a = dq + r}.$$

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**

Greatest common divisor

Definition: Let a and b are integers, not both 0. Then the largest integer d such that d | a and d | b is called **the greatest common divisor** of a and b. The greatest common divisor is denoted as gcd(a,b).

Examples:

- gcd(24,36) = ?

Greatest common divisor

Definition: Let a and b are integers, not both 0. Then the largest integer d such that d | a and d | b is called **the greatest common divisor** of a and b. The greatest common divisor is denoted as gcd(a,b).

Examples:

- gcd(24,36) = ?
- Check 2,3,4,6,12 gcd(24,36) = 12
- gcd(11,23) = ?

Greatest common divisor

Definition: Let a and b are integers, not both 0. Then the largest integer d such that d | a and d | b is called **the greatest common divisor** of a and b. The greatest common divisor is denoted as gcd(a,b).

Examples:

- gcd(24,36) = ?
- 12 (start with 2,3,4,6,12)
- gcd(11,23) = ?
- 2 ways: 1) Check 2,3,4,5,6 …
  2) 11 is a prime so only the multiples of it are possible
- no positive integer greater than 1 that divides both numbers

Greatest common divisor

A systematic way to find the gcd using factorization:

- Let $a=p_1^{a1}\ p_2^{a2}\ p_3^{a3} \ldots p_k^{ak}$ and $b= p_1^{b1}\ p_2^{b2}\ p_3^{b3} \ldots p_k^{bk}$
- $gcd(a,b)= p_1^{\min(a1,b1)}\ p_2^{\min(a2,b2)}\ p_3^{\min(a3,b3)} \ldots p_k^{\min(ak,bk)}$

Examples:

- gcd(24,36) = ?
- $24 = 2*2*2*3=2^3*3$
- $36= 2*2*3*3=2^2*3^2$
- gcd(24,36) =

Greatest common divisor

A systematic way to find the gcd using factorization:

- Let $a=p_1^{a1}\ p_2^{a2}\ p_3^{a3} \dots p_k^{ak}$ and $b= p_1^{b1}\ p_2^{b2}\ p_3^{b3} \dots p_k^{bk}$
- $gcd(a,b)= p_1^{\min(a1,b1)}\ p_2^{\min(a2,b2)}\ p_3^{\min(a3,b3)} \dots p_k^{\min(ak,bk)}$

Examples:

- gcd(24,36) = ?
- $24 = 2*2*2*3=2^3*3$
- $36= 2*2*3*3=2^2*3^2$
- $gcd(24,36) =2^2*3 =$ **12**

Least common multiple

Definition: Let a and b are two positive integers. The least common multiple of a and b is the smallest positive integer that is divisible by both a and b. The **least common multiple** is denoted as **lcm(a,b).**

Example:

- **What is lcm(12,9) =?**
- Give me a common multiple: …

Least common multiple

Definition: Let a and b are two positive integers. The least common multiple of a and b is the smallest positive integer that is divisible by both a and b. The **least common multiple** is denoted as **lcm(a,b).**

Example:

- **What is lcm(12,9) =?**
- Give me a common multiple: … 12*9= 108
- **Can we find a smaller number?**

Least common multiple

Definition: Let a and b are two positive integers. The least common multiple of a and b is the smallest positive integer that is divisible by both a and b. The **least common multiple** is denoted as **lcm(a,b).**

Example:

- **What is lcm(12,9) =?**
- Give me a common multiple: … 12*9= 108
- **Can we find a smaller number?**
- **Yes.** Try 36. Both 12 and 9 cleanly divide 36.

Least common multiple

A systematic way to find the lcm using factorization:

- Let $a=p_1^{a1} p_2^{a2} p_3^{a3} \dots p_k^{ak}$ and $b= p_1^{b1} p_2^{b2} p_3^{b3} \dots p_k^{bk}$
- $lcm(a,b)= p_1^{\max(a1,b1)} p_2^{\max(a2,b2)} p_3^{\max(a3,b3)} \dots p_k^{\max(ak,bk)}$

Example:

- **What is lcm(12,9) =?**
- $12 = 2*2*3=2^2*3$
- $9=3*3 =3^2$
- **lcm(12,9)** =

Least common multiple

A systematic way to find the lcm using factorization:

- Let $a=p_1^{a1} p_2^{a2} p_3^{a3} \dots p_k^{ak}$ and $b= p_1^{b1} p_2^{b2} p_3^{b3} \dots p_k^{bk}$
- $lcm(a,b)= p_1^{\max(a1,b1)} p_2^{\max(a2,b2)} p_3^{\max(a3,b3)} \dots p_k^{\max(ak,bk)}$

Example:

- **What is lcm(12,9) =?**
- $12 = 2*2*3=2^2*3$
- $9=3*3 =3^2$
- **lcm(12,9)** = $2^2 * 3^2 = 4 * 9 =$ **36**

Euclid algorithm

Finding the greatest common divisor requires factorization

- $a=p_1^{a1}\, p_2^{a2}\, p_3^{a3} \ldots p_k^{ak}$, $b= p_1^{b1}\, p_2^{b2}\, p_3^{b3} \ldots p_k^{bk}$
- $gcd(a,b)= p_1^{\min(a1,b1)}\, p_2^{\min(a2,b2)}\, p_3^{\min(a3,b3)} \ldots p_k^{\min(ak,bk)}$

- Factorization can be cumbersome and time consuming since we need to find all factors of the two integers that can be very large.

- Luckily a more efficient method for computing the gcd exists:
- It is called **Euclidean algorithm**
  - the method is known from ancient times and named after Greek mathematician Euclid.