ECEN 227 - Introduction to Finite Automata and Discrete Mathematics

Dr. Mahmoud Nabil
mnmahmoud@ncat.edu

North Carolina A & T State University

October 2, 2020

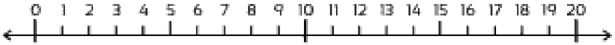
Talk Overview

1. The Division Algorithm
2. Modular Arithmetic
3. Prime factorizations
4. Primality Test

Outline

Number Theory Introduction

- Why do we use numbers basically?



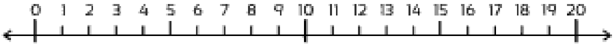
Ex.

$5+3 = 8$ $8\text{-}3 = 5$

$5\times 3 = 15$ $15\div 3 = 5$

Number Theory Introduction

- Why do we use numbers basically?
  - For Counting



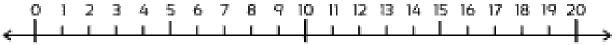
Ex.

$5+3 = 8$ 8-3 $= 5$

$5\times3 = 15$ $15\div3 = 5$

Number Theory Introduction

- Why do we use numbers basically?
  - For Counting
- Addition and Multiplication operations are invented to support fast counting



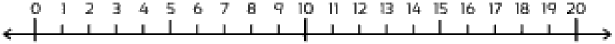
Ex.

$5+3 = 8$ $\qquad$ 8-3 $= 5$

$5\times3 = 15$ $\qquad$ $15\div3 = 5$

Number Theory Introduction

- Why do we use numbers basically?
  - For Counting
- Addition and Multiplication operations are invented to support fast counting
- Subtraction and Division are then introduced as inverse operations for Addition and Multiplication.



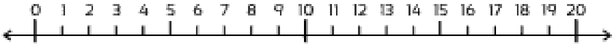
Ex.

$5+3 = 8$ $\qquad$ $8-3 = 5$

$5\times 3 = 15$ $\qquad$ $15\div 3 = 5$

Number Theory Introduction

- Why do we use numbers basically?
  - For Counting
- Addition and Multiplication operations are invented to support fast counting
- Subtraction and Division are then introduced as inverse operations for Addition and Multiplication.
- Operations are done on the number line.



Ex.

$5+3 = 8$ $8\text{-}3 = 5$

$5\times3 = 15$ $15\div3 = 5$

Division

- We will focus our study on division when investigating the properties of integers.
- As division is not always possible to result an integer. **Ex.** $9 \div 4 = 2.25$

Division

- We will focus our study on division when investigating the properties of integers.
- As division is not always possible to result an integer. **Ex.** $9 \div 4 = 2.25$
- Division is widely used in modern cryptography as an inverse operation for the multiplication.

Division

- We will focus our study on division when investigating the properties of integers.
- As division is not always possible to result an integer. **Ex.** $9 \div 4 = 2.25$
- Division is widely used in modern cryptography as an inverse operation for the multiplication.

Number theory

Number theory is a branch of mathematics concerned with the study of integers. It forms the mathematical basis for modern cryptography.

What is Division

- What does it means a is divisible by b?

What is Division

- What does it means a is divisible by b?
  - **A naive answer** if the rational number $\frac{a}{b}$ is an integer say k, then a is divisible by b.
- But what does it means $\frac{a}{b}$ is an integer?

What is Division

- What does it means a is divisible by b?
  - **A naive answer** if the rational number $\frac{a}{b}$ is an integer say k, then a is divisible by b.
- But what does it means $\frac{a}{b}$ is an integer?
  - It means a can be written as a product of two intgers one of them is b.

What is Division

- What does it means a is divisible by b?
  - **A naive answer** if the rational number $\frac{a}{b}$ is an integer say k, then a is divisible by b.
- But what does it means $\frac{a}{b}$ is an integer?
  - It means a can be written as a product of two intgers one of them is b.
  - Or, $a = k \times b$

What is Division

- What does it means a is divisible by b?
  - **A naive answer** if the rational number $\frac{a}{b}$ is an integer say k, then a is divisible by b.
- But what does it means $\frac{a}{b}$ is an integer?
  - It means a can be written as a product of two intgers one of them is b.
  - Or, $a = k \times b$
  - Then, $\frac{a}{b} = k$

What is Division

- What does it means a is divisible by b?
  - **A naive answer** if the rational number $\frac{a}{b}$ is an integer say k, then a is divisible by b.
- But what does it means $\frac{a}{b}$ is an integer?
  - It means a can be written as a product of two intgers one of them is b.
  - Or, $a = k \times b$
  - Then, $\frac{a}{b} = k$
  - We call b is factor or divisor of a.

What is Division

- What does it means a is divisible by b?
  - **A naive answer** if the rational number $\frac{a}{b}$ is an integer say k, then a is divisible by b.
- But what does it means $\frac{a}{b}$ is an integer?
  - It means a can be written as a product of two intgers one of them is b.
  - Or, a = k×b
  - Then, $\frac{a}{b} = k$
  - We call b is factor or divisor of a.

What is Division

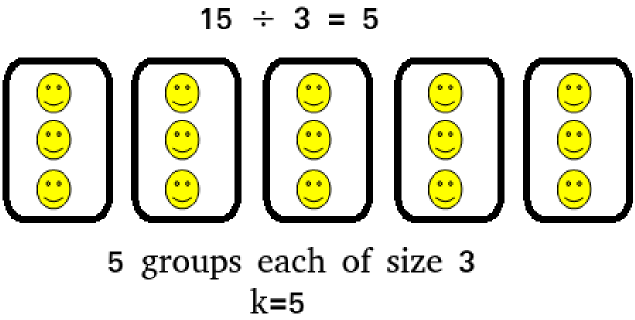
- What does it means a is divisible by b?
  - **A naive answer** if the rational number $\frac{a}{b}$ is an integer say k, then a is divisible by b.
- But what does it means $\frac{a}{b}$ is an integer?
  - It means a can be written as a product of two intgers one of them is b.
  - Or, a $=$ k$\times$b
  - Then, $\frac{a}{b} = k$
  - We call b is factor or divisor of a.

Divisibality

a is divisible by b (or b divides a) denoted by $b \mid a$ if there is an integer k such that $a = k \times b$

Divisibality

- $b \mid a$ read as b divides a.
- a can be divided into k groups each of size b if the division is possible.



Excercise

Indicate whether each expression is true or false.

- $8 \mid 40$

Excercise

Indicate whether each expression is true or false.

- $8 \mid 40$
  - True

Excercise

Indicate whether each expression is true or false.

- $8 \mid 40$
  - True
- $7 \mid 50$

Excercise

Indicate whether each expression is true or false.

- $8 \mid 40$
  - True
- $7 \mid 50$
  - False

Excercise

Indicate whether each expression is true or false.

- $8 \mid 40$
  - True
- $7 \mid 50$
  - False
- $6 \nmid 36$

Excercise

Indicate whether each expression is true or false.

- $8 \mid 40$
  - True
- $7 \mid 50$
  - False
- $6 \nmid 36$
  - False

Excercise

Indicate whether each expression is true or false.

- $8 \mid 40$
  - True
- $7 \mid 50$
  - False
- $6 \nmid 36$
  - False
- $-2 \mid 10$

Excercise

Indicate whether each expression is true or false.

- $8 \mid 40$
  - True
- $7 \mid 50$
  - False
- $6 \nmid 36$
  - False
- $-2 \mid 10$
  - True

Excercise

Indicate whether each expression is true or false.

- $8 \mid 40$
  - True
- $7 \mid 50$
  - False
- $6 \nmid 36$
  - False
- $-2 \mid 10$
  - True
- $3 \mid -10$

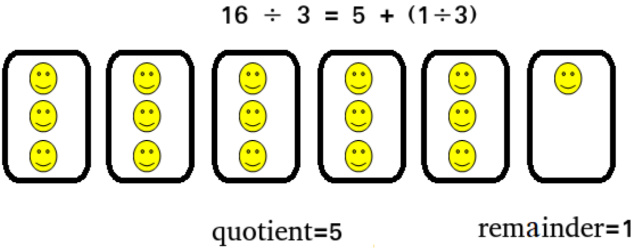
Excercise

Indicate whether each expression is true or false.

- $8 \mid 40$
  - True
- $7 \mid 50$
  - False
- $6 \nmid 36$
  - False
- $-2 \mid 10$
  - True
- $3 \mid -10$
  - False

Divisibality

- What if b can not divided a?



The division algorithm

Theorem

Let n be an integer and let d be a positive integer. Then, there are unique integers q and r, with $0 \leq r \leq d - 1$, such that $n = qd + r$.

Ex.

- $\frac{16}{3} \Rightarrow 16 = 5(3)\ +1$

The division algorithm

Theorem

Let n be an integer and let d be a positive integer. Then, there are unique integers q and r, with $0 \le r \le d - 1$, such that $n = qd + r$.

Ex.

- $\frac{16}{3} \Rightarrow 16 = 5(3) + 1$
- quotient $= 5$ and remainder $= 1$

The division algorithm

Theorem

Let n be an integer and let d be a positive integer. Then, there are unique integers q and r, with $0 \leq r \leq d - 1$, such that $n = qd + r$.

Ex.

- $\frac{16}{3} \Rightarrow 16 = 5(3) + 1$
- quotient $= 5$ and remainder $= 1$

The division algorithm

Theorem

Let n be an integer and let d be a positive integer. Then, there are unique integers q and r, with $0 \leq r \leq d - 1$, such that $n = qd + r$.

Ex.

- $\frac{16}{3} \Rightarrow 16 = 5(3)\ +1$
- quotient $= 5$ and remainder $= 1$
- $\frac{-16}{3} \Rightarrow -16 = (-6)(3)\ \ +2$

The division algorithm

Theorem

Let n be an integer and let d be a positive integer. Then, there are unique integers q and r, with $0 \leq r \leq d - 1$, such that $n = qd + r$.

Ex.

- $\frac{16}{3} \Rightarrow 16 = 5(3) + 1$
- quotient = 5 and remainder = 1
- $\frac{-16}{3} \Rightarrow -16 = (-6)(3) + 2$
- quotient = -6 and remainder = 2

The division algorithm

Theorem

Let n be an integer and let d be a positive integer. Then, there are unique integers q and r, with $0 \leq r \leq d - 1$*, such that* $n = qd + r$.

Ex.

- $\frac{16}{3} \Rightarrow 16 = 5(3) + 1$
- quotient = 5 and remainder = 1
- $\frac{-16}{3} \Rightarrow -16 = (-6)(3) + 2$
- quotient = -6 and remainder = 2

The division algorithm

Theorem

Let n be an integer and let d be a positive integer. Then, there are unique integers q and r, with $0 \leq r \leq d - 1$, such that $n = qd + r$.

Ex.

- $\frac{16}{3} \Rightarrow 16 = 5(3) + 1$
- quotient $= 5$ and remainder $= 1$
- $\frac{-16}{3} \Rightarrow -16 = (-6)(3) \; +2$
- quotient $=$ -6 and remainder $= 2$

We say

- 16 div 3 $= 5$ (quotient)

The division algorithm

Theorem

Let n be an integer and let d be a positive integer. Then, there are unique integers q and r, with $0 \leq r \leq d - 1$, such that $n = qd + r$.

Ex.

- $\frac{16}{3} \Rightarrow 16 = 5(3) + 1$
- quotient $= 5$ and remainder $= 1$
- $\frac{-16}{3} \Rightarrow -16 = (-6)(3) + 2$
- quotient $=$ -6 and remainder $= 2$

We say

- 16 div 3 $= 5$ (quotient)
- 16 mod 3 $= 1$ (remainder)

The division algorithm

Theorem

Let n be an integer and let d be a positive integer. Then, there are unique integers q and r, with $0 \leq r \leq d - 1$, such that $n = qd + r$.

Ex.

- $\frac{16}{3} \Rightarrow 16 = 5(3)\ +1$
- quotient $= 5$ and remainder $= 1$
- $\frac{-16}{3} \Rightarrow -16 = (-6)(3)\ \ +2$
- quotient $=$ -6 and remainder $= 2$

We say

- 16 div $3 = 5$ (quotient)
- $16 \bmod 3 = 1$ (remainder)

The division algorithm

Theorem

Let n be an integer and let d be a positive integer. Then, there are unique integers q and r, with $0 \leq r \leq d - 1$, such that $n = qd + r$.

Ex.

- $\frac{16}{3} \Rightarrow 16 = 5(3) +1$
- quotient $=$ 5 and remainder $=$ 1
- $\frac{-16}{3} \Rightarrow -16 = (-6)(3) \ +2$
- quotient $=$ -6 and remainder $=$ 2

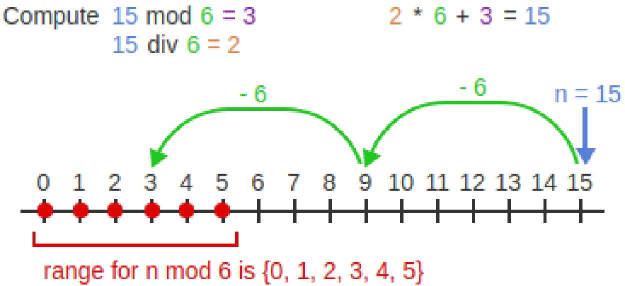
We say

- 16 div 3 $=$ 5 (quotient)
- 16 mod 3 $=$ 1 (remainder)

Note that

We are dealing with positive divisors, thus the remainder is always positive

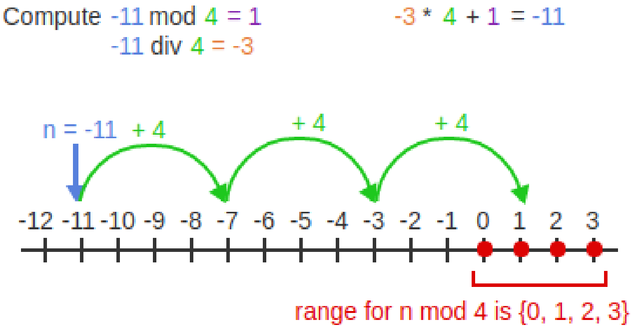
Computing div and mod.



Note that

Remainder is always positive i.e., $0 \leq r \leq d - 1$

Computing div and mod for positive number.



Note that

Remainder is always positive i.e., $0 \leq r \leq d - 1$

Excercise

1. 344 mod 5

Excercise

1. 344 mod 5
   - $344 = 68 \times 5 + 4$, so $344 \bmod 5 = 4$.
2. 344 div 5

Excercise

1. 344 mod 5
    - $344 = 68 \times 5 + 4$, so 344 mod 5 = 4.
2. 344 div 5
    - $344 = 68 \times 5 + 4$, so 344 div 5 = 68.
3. -344 mod 5

Excercise

1. 344 mod 5
   - $344 = 68 \times 5 + 4$, so 344 mod 5 $= 4$.
2. 344 div 5
   - $344 = 68 \times 5 + 4$, so 344 div 5 $= 68$.
3. -344 mod 5
   - $(-344) = (-69) \times 5 + 1$, so (-344) mod 5 $= 1$.
4. -344 div 5

Excercise

1. 344 mod 5
   - $344 = 68 \times 5 + 4$, so $344 \text{ mod } 5 = 4$.
2. 344 div 5
   - $344 = 68 \times 5 + 4$, so $344 \text{ div } 5 = 68$.
3. -344 mod 5
   - $(-344) = (-69) \times 5 + 1$, so $(-344) \text{ mod } 5 = 1$.
4. -344 div 5
   - $(-344) = (-69) \times 5 + 1$, so $(-344) \text{ div } 5 = -69$.

Excercise

Determine the value of n based on the given information.

- n div $7 = 11$, n mod $7 = 5$

Excercise

Determine the value of n based on the given information.

- n div 7 = 11, n mod 7 = 5
  - n=11*7+5=82

Excercise

Determine the value of n based on the given information.

- n div 7 = 11, n mod 7 = 5
  - n=11*7+5=82
- n div 5 = -10, n mod 5 = 4

Excercise

Determine the value of n based on the given information.

- n div 7 = 11, n mod 7 = 5
  - n=11*7+5=82
- n div 5 = -10, n mod 5 = 4
  - n=-10*5+4=-46

Excercise

Determine the value of n based on the given information.

- n div 7 = 11, n mod 7 = 5
  - n=11*7+5=82
- n div 5 = -10, n mod 5 = 4
  - n=-10*5+4=-46
- n div 10 = 2, n mod 10 = 8

Excercise

Determine the value of n based on the given information.

- n div 7 = 11, n mod 7 = 5
  - n=11*7+5=82
- n div 5 = -10, n mod 5 = 4
  - n=-10*5+4=-46
- n div 10 = 2, n mod 10 = 8
  - n= 10*2+8

Excercise

Determine the value of n based on the given information.

- n div 7 = 11, n mod 7 = 5
  - n=11*7+5=82
- n div 5 = -10, n mod 5 = 4
  - n=-10*5+4=-46
- n div 10 = 2, n mod 10 = 8
  - n= 10*2+8
- n div 11 = -3, n mod 11 = 7

Excercise

Determine the value of n based on the given information.

- n div 7 = 11, n mod 7 = 5
  - n=11*7+5=82
- n div 5 = -10, n mod 5 = 4
  - n=-10*5+4=-46
- n div 10 = 2, n mod 10 = 8
  - n= 10*2+8
- n div 11 = -3, n mod 11 = 7
  - n= 11*(-3)+7=-26

Excercise

- For which values of n is n div $7 = 3$?

Excercise

- For which values of n is n div 7 = 3?
  - n = 3 * 7 + r, for any integer r in the range from 0 through 6.
    n = 21, 22, 23, 24, 25, 26, and 27.

Excercise

- For which values of n is n div $7 = 3$?
  - $n = 3 * 7 + r$, for any integer r in the range from 0 through 6.
    $n = 21, 22, 23, 24, 25, 26$, and 27.
- For which values of n is n div $4 = 2$?

Excercise

- For which values of n is n div 7 = 3?
  - n = 3 * 7 + r, for any integer r in the range from 0 through 6.
    n = 21, 22, 23, 24, 25, 26, and 27.
- For which values of n is n div 4 = 2?
  - n = 2 * 4 + r, for any integer r in the range from 0 through 3.
    n = 8, 9, 10, 11.

Excercise

- For which values of n is n div 7 = 3?
  - n = 3 * 7 + r, for any integer r in the range from 0 through 6. n = 21, 22, 23, 24, 25, 26, and 27.
- For which values of n is n div 4 = 2?
  - n = 2 * 4 + r, for any integer r in the range from 0 through 3. n = 8, 9, 10, 11.
- For which values of n is n div 5 = -6?

Excercise

- For which values of n is n div 7 = 3?
  - n = 3 * 7 + r, for any integer r in the range from 0 through 6. n = 21, 22, 23, 24, 25, 26, and 27.
- For which values of n is n div 4 = 2?
  - n = 2 * 4 + r, for any integer r in the range from 0 through 3. n = 8, 9, 10, 11.
- For which values of n is n div 5 = -6?
  - n = -6 * 5 + r, for any integer r in the range from 0 through 4. n = -30, -29, -28, -27, and -26.

Divisibility and linear combinations

- A linear combination of two numbers is the sum of multiples of those numbers. For example, $3x - 7y$ and $-2x + 4y$ are both linear combinations of x and y.

Divisibility and linear combinations

- A linear combination of two numbers is the sum of multiples of those numbers. For example, 3x - 7y and -2x + 4y are both linear combinations of x and y.

Theorem

if z divides x (i.e., $z \mid x$) and z divides y (i.e., $z \mid y$), then z divides any linear combination of x and y (i.e., $z \mid ax+by$).

Divisibility and linear combinations

- A linear combination of two numbers is the sum of multiples of those numbers. For example, 3x - 7y and -2x + 4y are both linear combinations of x and y.

Theorem

if z divides x (i.e., $z \mid x$) and z divides y (i.e., $z \mid y$), then z divides any linear combination of x and y (i.e., $z \mid ax+by$).

Ex.

if 2 divides 10 and 2 divdes 20

Then 2 divdes any number in the form 10a+20b for any a and b.

Excercise

- Does 6 divides 462 given that the number 462 is a linear combination of 12 and 18 ($19*12 + 13*18 = 462$).

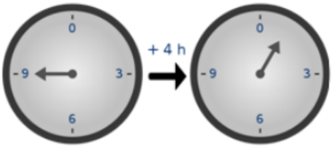
Excercise

- Does 6 divides 462 given that the number 462 is a linear combination of 12 and 18 ($19*12 + 13*18 = 462$).
  - Yes

Outline

Modular Arithmetic

- In modular arithmetic, numbers "wrap around" upon reaching a given fixed quantity (this given quantity is known as the modulus) to leave a remainder.
- Imagine we are doing the arithmetic on circle instead of the number line.
- In modulo N, the result of any arithmetic operation takes values from 0 to N-1.



The 12-hour clock : **modulo 12**
If the time is 9:00 now, then 4 hours later it will be 1:00

9+4 =13
13 % 12= 1

Modular Arithmetic

- 1:00 and 13:00 hours are the same
- 1:00 and 25:00 hours are the same
- $1 \equiv 13 \mod 12$
- $13 \equiv 25 \mod 12$

$$a \equiv b \mod n$$

- n is the modulus
- a is congruent to b modulo n
- $a \mod n = b \mod n$
- a-b is an integer multiple of n (i.e., $n \mid (a-b)$)

Example

- $38 \equiv 14 \mod 12$

Example

- $38 \equiv 14 \bmod 12$
  - 38-14 $= 24$; multiple of 12
- $38 \equiv 2 \bmod 12$

Example

- $38 \equiv 14 \bmod 12$
  - $38\text{-}14 = 24$; multiple of 12
- $38 \equiv 2 \bmod 12$
  - $38\text{-}2 = 36$; multiple of 12

The same rule apply for negative numbers.

- $-8 \equiv 7 \bmod 5$

Example

- $38 \equiv 14 \bmod 12$
  - 38-14 $=$ 24; multiple of 12
- $38 \equiv 2 \bmod 12$
  - 38-2 $=$ 36; multiple of 12

The same rule apply for negative numbers.

- $-8 \equiv 7 \bmod 5$
- $2 \equiv -3 \bmod 5$

Example

- $38 \equiv 14 \bmod 12$
  - 38-14 = 24; multiple of 12
- $38 \equiv 2 \bmod 12$
  - 38-2 = 36; multiple of 12

The same rule apply for negative numbers.

- $-8 \equiv 7 \bmod 5$
- $2 \equiv -3 \bmod 5$
- $-3 \equiv -8 \bmod 5$

Example

- $38 \equiv 14 \bmod 12$
  - $38\text{-}14 = 24$; multiple of 12
- $38 \equiv 2 \bmod 12$
  - $38\text{-}2 = 36$; multiple of 12

The same rule apply for negative numbers.

- $-8 \equiv 7 \bmod 5$
- $2 \equiv -3 \bmod 5$
- $-3 \equiv -8 \bmod 5$

Congruence Class Example

Integers modulo 5 can take values from $\{0, 1, 2, 3, 4\}$

$0 \equiv 5 \equiv 10 \equiv 15 \ldots \mod 5$
$1 \equiv 6 \equiv 11 \equiv 16 \ldots \mod 5$
$2 \equiv 7 \equiv 12 \equiv 17 \ldots \mod 5$
$3 \equiv 8 \equiv 13 \equiv 18 \ldots \mod 5$
$4 \equiv 9 \equiv 14 \equiv 19 \ldots \mod 5$

We call the previous property as congruence class relation modulo 5.

Ring

Ring

The set {0, 1, 2,..., m-1} along with addition and multiplication mod m defines a closed mathematical system with m elements called a ring Z_m.

Ex.

Ring

Ring

The set $\{0, 1, 2, \ldots, m\text{-}1\}$ along with addition and multiplication mod m defines a closed mathematical system with m elements called a ring Z_m.

Ex.

- The set $Z_{13} = \{0, 1, 2, \ldots, 12\}$ is an arithmetic system modulo 13.
- The set $Z_{17} = \{0, 1, 2, \ldots, 16\}$ is an arithmetic system modulo 17.

Modular Arithmetic Operations

Addition

$[x + y] \text{ mod } m = [(x \text{ mod } m) + (y \text{ mod } m)] \text{ mod } m$

Multiplication

$[x * y] \text{ mod } m = [(x \text{ mod } m) * (y \text{ mod } m)] \text{ mod } m$

Exponentiation

$x^n \text{ mod } m = [(x \text{ mod } m)^n] \text{ mod } m$

Excercise 1

Calculate the following:

- $(72 \times (\text{-}65) + 211) \bmod 7$

Excercise 1

Calculate the following:

- $(72 \times (\text{-}65) + 211) \bmod 7$
  - $(72 \times (\text{-}65) + 211) \bmod 7 = ((72 \bmod 7) \times (\text{-}65 \bmod 7) + (211 \bmod 7)) \bmod 7 = (2 \times 5 + 1) \bmod 7 = 11 \bmod 7 = 4$

Excercise 1

Calculate the following:

- $(72 \times (\text{-}65) + 211) \bmod 7$
  - $(72 \times (\text{-}65) + 211) \bmod 7 = ((72 \bmod 7) \times (\text{-}65 \bmod 7) + (211 \bmod 7)) \bmod 7 = (2 \times 5 + 1) \bmod 7 = 11 \bmod 7 = 4$
- $38^7 \bmod 3$

Excercise 1

Calculate the following:

- $(72 \times (\text{-}65) + 211) \bmod 7$
  - $(72 \times (\text{-}65) + 211) \bmod 7 = ((72 \bmod 7) \times (\text{-}65 \bmod 7) + (211 \bmod 7)) \bmod 7 = (2 \times 5 + 1) \bmod 7 = 11 \bmod 7 = 4$
- $38^7 \bmod 3$
  - $(38 \bmod 3)^7 = (2 \bmod 3)^7 = (2 \bmod 3)^5 * (2 \bmod 3)^2 = (32 \bmod 3) * (4 \bmod 3) = 2 \bmod 3$

Excercise 1

Calculate the following:

- (72 × (-65) + 211) mod 7
  - (72 × (-65) + 211) mod 7 = ((72 mod 7) × (-65 mod 7) + (211 mod 7)) mod 7 = (2 × 5 + 1) mod 7 = 11 mod 7 = 4
- 38^7 mod 3
  - $(38 \bmod 3)^7 = (2 \bmod 3)^7 = (2 \bmod 3)^5 * (2 \bmod 3)^2 =$ $(32 \bmod 3) * (4 \bmod 3) = 2 \bmod 3$
- 44^{12} mod 6

Excercise 1

Calculate the following:

- $(72 \times \text{(-65)} + 211) \text{ mod } 7$
  - $(72 \times \text{(-65)} + 211) \text{ mod } 7 = ((72 \text{ mod } 7) \times (\text{-65 mod } 7) + (211 \text{ mod } 7)) \text{ mod } 7 = (2 \times 5 + 1) \text{ mod } 7 = 11 \text{ mod } 7 = 4$
- $38^7 \text{ mod } 3$
  - $(38 \text{ mod } 3)^7 = (2 \text{ mod } 3)^7 = (2 \text{ mod } 3)^5 * (2 \text{ mod } 3)^2 = (32 \text{ mod } 3) * (4 \text{ mod } 3) = 2 \text{ mod } 3$
- $44^{12} \text{ mod } 6$
  - $(44 \text{ mod } 6)^{12} = (2 \text{ mod } 6)^{12} = (2^6 \text{ mod } 6)^2 = (64 \text{ mod } 6)^2 = (4 \text{ mod } 6)^2 = 4$

Excercise 1

Calculate the following:

- $(72 \times (\text{-}65) + 211) \bmod 7$
  - $(72 \times (\text{-}65) + 211) \bmod 7 = ((72 \bmod 7) \times (\text{-}65 \bmod 7) + (211 \bmod 7)) \bmod 7 = (2 \times 5 + 1) \bmod 7 = 11 \bmod 7 = 4$
- $38^7 \bmod 3$
  - $(38 \bmod 3)^7 = (2 \bmod 3)^7 = (2 \bmod 3)^5 * (2 \bmod 3)^2 = (32 \bmod 3) * (4 \bmod 3) = 2 \bmod 3$
- $44^{12} \bmod 6$
  - $(44 \bmod 6)^{12} = (2 \bmod 6)^{12} = (2^6 \bmod 6)^2 = (64 \bmod 6)^2 = (4 \bmod 6)^2 = 4$
- $46^{30} \bmod 9$

Excercise 1

Calculate the following:

- $(72 \times (\text{-}65) + 211) \bmod 7$
  - $(72 \times (\text{-}65) + 211) \bmod 7 = ((72 \bmod 7) \times (\text{-}65 \bmod 7) + (211 \bmod 7)) \bmod 7 = (2 \times 5 + 1) \bmod 7 = 11 \bmod 7 = 4$
- $38^7 \bmod 3$
  - $(38 \bmod 3)^7 = (2 \bmod 3)^7 = (2 \bmod 3)^5 * (2 \bmod 3)^2 = (32 \bmod 3) * (4 \bmod 3) = 2 \bmod 3$
- $44^{12} \bmod 6$
  - $(44 \bmod 6)^{12} = (2 \bmod 6)^{12} = (2^6 \bmod 6)^2 = (64 \bmod 6)^2 = (4 \bmod 6)^2 = 4$
- $46^{30} \bmod 9$
  - $(46 \bmod 9)^{30} \bmod 9 = (1^{30}) \bmod 9 = 1 \bmod 9 = 1$

Excercise 2

Compute $3^{1000} \bmod 7$

Excercise 2

Compute $3^{1000} \bmod 7$

3^{1000} is hard to compute by hand but can we learn anything from trying small modular exponents of 3? (You can use calculator)

Excercise 2

Compute $3^{1000} \bmod 7$

3^{1000} is hard to compute by hand but can we learn anything from trying small modular exponents of 3? (You can use calculator)

Excercise 2

Compute 3^{1000} mod 7

3^{1000} is hard to compute by hand but can we learn anything from trying small modular exponents of 3? (You can use calculator)

3^1 mod 7 $=$3

Excercise 2

Compute $3^{1000} \bmod 7$

3^{1000} is hard to compute by hand but can we learn anything from trying small modular exponents of 3? (You can use calculator)

$3^1 \bmod 7 = 3$

$3^2 \bmod 7 = 2$

Excercise 2

Compute $3^{1000} \bmod 7$

3^{1000} is hard to compute by hand but can we learn anything from trying small modular exponents of 3? (You can use calculator)

$3^1 \bmod 7 = 3$

$3^2 \bmod 7 = 2$

$3^3 \bmod 7 = 6$

Excercise 2

Compute $3^{1000} \bmod 7$

3^{1000} is hard to compute by hand but can we learn anything from trying small modular exponents of 3? (You can use calculator)

$3^1 \bmod 7 = 3$

$3^2 \bmod 7 = 2$

$3^3 \bmod 7 = 6$

$3^4 \bmod 7 = 4$

Excercise 2

Compute $3^{1000} \bmod 7$

3^{1000} is hard to compute by hand but can we learn anything from trying small modular exponents of 3? (You can use calculator)

$3^1 \bmod 7 = 3$

$3^2 \bmod 7 = 2$

$3^3 \bmod 7 = 6$

$3^4 \bmod 7 = 4$

$3^5 \bmod 7 = 5$

Excercise 2

Compute 3^{1000} mod 7

3^{1000} is hard to compute by hand but can we learn anything from trying small modular exponents of 3? (You can use calculator)

3^1 mod 7 $=3$

3^2 mod 7 $=2$

3^3 mod 7 $=6$

3^4 mod 7 $=4$

3^5 mod 7 $=5$

3^6 mod 7 $=1$

$$
\begin{aligned}
3^{1000}\ mod\ 7 &= 3^{6*166+4}\ mod\ 7 \\
&= [3^{6*166}\ mod\ 7 \times 3^4\ mod\ 7]\ mod\ 7 \\
&= [[3^6\ mod\ 7]^{166}\ mod\ 7] \times [3^4\ mod\ 7]\ mod\ 7 \\
&= [[1\ mod\ 7]^{166}\ mod\ 7] \times [3^4\ mod\ 7]\ mod\ 7 \\
&= 1 \times [3^4\ mod\ 7]\ mod\ 7 \\
&= 4
\end{aligned}
$$

Outline

Prime VS Composite Numbers

Prime Number

A prime number p is an integer that can be divided, without a remainder, only by itself and by 1.

Ex.

2,3,5,7,11,13

Composite Number

A positive integer is composite if it has a factor/divisor other than 1 or itself.

Ex.

$14 = 2 \times 7$
$10 = 2 \times 5$
$35 = 5 \times 7$

The Fundamental Theorem of Arithmetic

Theorem

Every positive integer other than 1 can be expressed uniquely as a product of prime numbers where the prime factors are written in increasing order.

Ex.

$1078 = 2 \times 7^2 \times 11$

The factors of 1078 are 2, 7, 11

- The multiplicity of 2 is 1
- The multiplicity of 7 is 2
- The multiplicity of 11 is 1

Excercise

Give the prime factorization for each number.

- 32

Excercise

Give the prime factorization for each number.

- 32
    - 2^5

Excercise

Give the prime factorization for each number.

- 32
  - 2^5
- 42

Excercise

Give the prime factorization for each number.

- 32
  - 2^5
- 42
  - $2 \times 3 \times 7$

Excercise

Give the prime factorization for each number.

- 32
  - 2^5
- 42
  - $2 \times 3 \times 7$
- 84

Excercise

Give the prime factorization for each number.

- 32
    - 2^5
- 42
    - $2 \times 3 \times 7$
- 84
    - $2^2 \times 3 \times 7$

Excercise

Give the prime factorization for each number.

- 32
  - 2^5
- 42
  - $2 \times 3 \times 7$
- 84
  - $2^2 \times 3 \times 7$
- 36

Excercise

Give the prime factorization for each number.

- 32
  - 2^5
- 42
  - $2 \times 3 \times 7$
- 84
  - $2^2 \times 3 \times 7$
- 36
  - $2^2 \times 3^2$

Greatest common divisor

GCD

The greatest common divisor (gcd) of non-zero integers x and y is the largest positive integer that is a factor of both x and y.

Ex.

GCD of 12 and 30

- Divisors of 12 are: 1, 2, 3, 4, **6** and 12

Greatest common divisor

GCD

The greatest common divisor (gcd) of non-zero integers x and y is the largest positive integer that is a factor of both x and y.

Ex.

GCD of 12 and 30

- Divisors of 12 are: 1, 2, 3, 4, **6** and 12
- Divisors of 30 are: 1, 2, 3, 5, **6**, 10, 15 and 30

Greatest common divisor

GCD

The greatest common divisor (gcd) of non-zero integers x and y is the largest positive integer that is a factor of both x and y.

Ex.

GCD of 12 and 30

- Divisors of 12 are: 1, 2, 3, 4, **6** and 12
- Divisors of 30 are: 1, 2, 3, 5, **6**, 10, 15 and 30

Greatest common divisor

GCD

The greatest common divisor (gcd) of non-zero integers x and y is the largest positive integer that is a factor of both x and y.

Ex.

GCD of 12 and 30

- Divisors of 12 are: 1, 2, 3, 4, **6** and 12
- Divisors of 30 are: 1, 2, 3, 5, **6**, 10, 15 and 30

The **Greatest Common Divisor** of 12 and 30 is **6**.

Least Common Multiple

LCM

The least common multiple (lcm) of non-zero integers x and y is the smallest positive integer that is an integer multiple of both x and y.

Ex.

LCM of 3 and 5:

- The multiples of 3 are: 3, 6, 9, 12, **15**, 18, ... etc

Least Common Multiple

LCM

The least common multiple (lcm) of non-zero integers x and y is the smallest positive integer that is an integer multiple of both x and y.

Ex.

LCM of 3 and 5:

- The multiples of 3 are: 3, 6, 9, 12, **15**, 18, ... etc
- The multiples of 5 are: 5, 10, **15**, 20, 25, ... etc

Least Common Multiple

LCM

The least common multiple (lcm) of non-zero integers x and y is the smallest positive integer that is an integer multiple of both x and y.

Ex.

LCM of 3 and 5:

- The multiples of 3 are: 3, 6, 9, 12, **15**, 18, ... etc
- The multiples of 5 are: 5, 10, **15**, 20, 25, ... etc

Least Common Multiple

LCM

The least common multiple (lcm) of non-zero integers x and y is the smallest positive integer that is an integer multiple of both x and y.

Ex.

LCM of 3 and 5:

- The multiples of 3 are: 3, 6, 9, 12, **15**, 18, ... etc
- The multiples of 5 are: 5, 10, **15**, 20, 25, ... etc

The **Least Common Multiple** of 3 and 5 is **15**

Calculating GCD and LCM Using Prime Factors

Let x and y be two positive integers with prime factorizations expressed using a common set of primes as:

$$x = p_1^{a_1} \times p_2^{a_2} \times \dots p_n^{a_n}$$

$$y = p_1^{b_1} \times p_2^{b_2} \times \dots p_n^{b_n}$$

$$\mathrm{GCD}(x\ ,\ y) = p_1^{min(a_1,b_1)} \times p_2^{min(a_2,b_2)} \times \dots p_n^{min(a_n,b_n)}$$

$$\mathrm{LCM}(x\ ,\ y) = p_1^{max(a_1,b_1)} \times p_2^{max(a_2,b_2)} \times \dots p_n^{max(a_n,b_n)}$$

Excercise

Some numbers and their prime factorizations are given below.

- $532 = 2^2 \times 7 \times 19$
- $648 = 2^3 \times 3^4$
- $1083 = 3 \times 19^2$
- $15435 = 3^2 \times 5 \times 7^3$

Use these prime factorizations to compute the following quantities.

1. gcd(532, 15435)
2. gcd(648, 1083)
3. lcm(532, 1083)
4. lcm(1083, 15435)

Outline

Checking a number is prime

- Primality test is an approach used to determine if a number **N** is prime.

Checking a number is prime

- Primality test is an approach used to determine if a number **N** is prime.

1. Iterate over numbers from 2 to N-1

Checking a number is prime

- Primality test is an approach used to determine if a number **N** is prime.

1. Iterate over numbers from 2 to N-1
2. If N is not divisible by any of these numbers then N is prime

Checking a number is prime

- Primality test is an approach used to determine if a number **N** is prime.

1. Iterate over numbers from 2 to N-1
2. If N is not divisible by any of these numbers then N is prime

Checking a number is prime

- Primality test is an approach used to determine if a number **N** is prime.

1. Iterate over numbers from 2 to N-1
2. If N is not divisible by any of these numbers then N is prime

Ex.

- How many checks you have to do to check if 23 is prime?
- 21 checks.

Checking a number is prime

Theorem

If N is a composite number, then N has a factor greater than 1 and at most $\sqrt{N}$

Checking a number is prime

Theorem

If N is a composite number, then N has a factor greater than 1 and at most $\sqrt{N}$

1. Iterate over numbers from 2 to $\sqrt{N}$
2. If N is not divisible by any of these numbers then N is prime

Ex.

- How many checks you have to do to check if 23 is prime using this theorem?
- $\sqrt{23}$ checks ≈ 5.
- very efficient if N is large

The Prime Number Theorem

Theorem

let $\pi(x)$ be the number of prime numbers in the range from 2 through x. Then

$$\lim_{x\to\infty} \frac{\pi(x)}{x/ln(x)} = 1$$

Ex

Excercise

Consider a random integer selected from the range from 2 to 1,000,000,000,000. Approximately, what are the chances that the selected number is prime?

Questions