ECEN 227 - Introduction to Finite Automata and Discrete Mathematics

Dr. Mahmoud Nabil
mnmahmoud@ncat.edu

North Carolina A & T State University

October 11, 2019

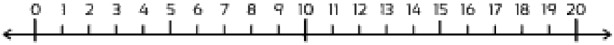
Talk Overview

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

Outline

Number Theory Introduction

- Why do we use numbers basically? 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.

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

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

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, 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, then a is divisible by b.
- But what does it means $\frac{a}{b}$ is an integer?
  - It means a can be as a product of two intgers one of them is b.
  - Or, $a = k \times b$
  - Then, $\frac{a}{b} = \frac{k \times b}{b} = k$
  - We call b is factor or divisor of a.

What is Division

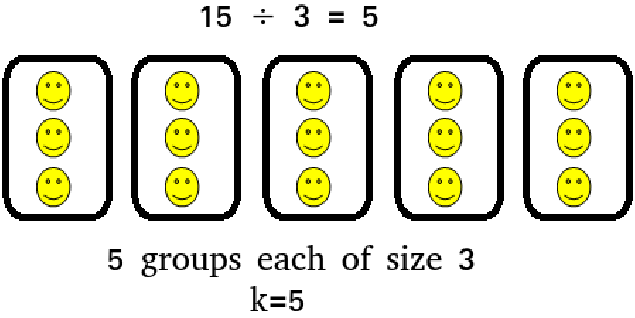
- What does it means a is divisible by b?
  - **A naive answer** if the rational number $\frac{a}{b}$ is an integer, then a is divisible by b.
- But what does it means $\frac{a}{b}$ is an integer?
  - It means a can be as a product of two intgers one of them is b.
  - Or, a = k×b
  - Then, $\frac{a}{b}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

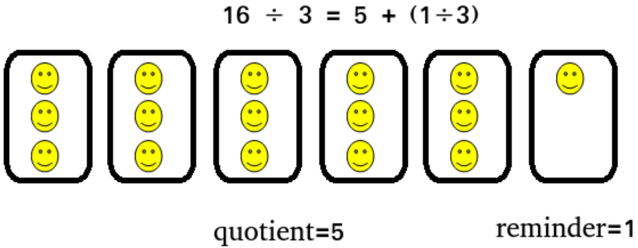
Divisibality

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



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 $0 \le r \le d - 1$, *such that* $n = qd + r$.

Ex.

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

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

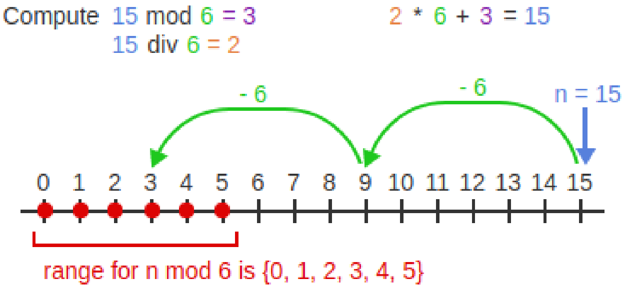
We say

- $16 \text{ div } 3 = 5$ (quotient)
- $16 \bmod 3 = 1$ (reminder)

Note that

Reminder is always positive

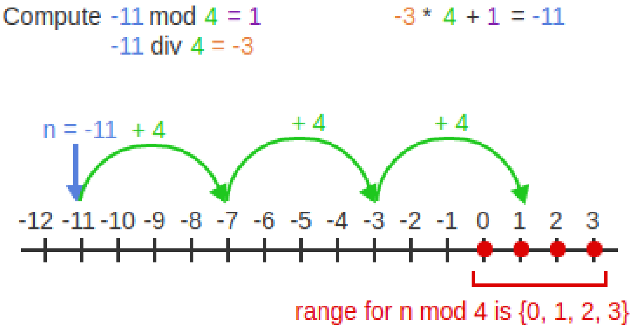
Computing div and mod.



Note that

Reminder is always positive

Computing div and mod for positive number.



Note that

Reminder is always positive

Computing div and mod for negative number.

Input: Integers n and d > 0.
Output: q = n div d, and r = n mod d.

Case 1: n ≥ 0.	Case 2: n < 0.

q := 0
r := n
While (r ≥ d)
    q := q + 1
    r := r - d
End-While
	q := 0
	r := n
	While (r < 0)
	    q := q - 1
	    r := r + d
	End-While

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

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 $344 \bmod 5 = 4$.
2. 344 div 5
   - $344 = 68 \times 5 + 4$, so $344 \operatorname{div} 5 = 68$.
3. -344 mod 5

Excercise

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

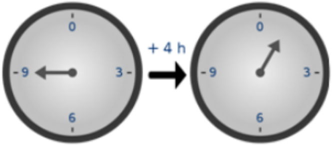
Excercise

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

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
- $1 \equiv 13 \bmod 12$
- $13 \equiv 25 \bmod 12$

$$a \equiv b \bmod n$$

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

Example

- $38 \equiv 14 \mod 12$

Example

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

Example

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

The same rule apply for negative numbers.

- $\text{-}8 \equiv 7 \bmod 5$

Example

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

The same rule apply for negative numbers.

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

Example

- $38 \equiv 14 \bmod 12$
  - 38-14 $=$ 12; 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

- $38 \equiv 14 \bmod 12$
  - $38\text{-}14 = 12$; 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 $\{0, 1, 2, 3, 4\}$

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

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

Ring

Ring

The set $\{0, 1, 2, \ldots, m-1\}$ 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 $\{0, 1, 2, \ldots, m-1\}$ 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

$[x + y] \bmod m = [(x \bmod m) + (y \bmod m)] \bmod m$

Multiplication

$[x * y] \bmod m = [(x \bmod m) * (y \bmod m)] \bmod m$

Exponentiation

$x^n \bmod m = [(x \bmod m)^n] \bmod m$

Excercise 1

Calculate the following:

- $(72 \times (65) + 211) \bmod 7$
- $38^7 \bmod 3$
- $44^{12} \bmod 6$

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

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
- 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:

$$x = p_1^{a_1} \times p_2^{a_2} \times \dots p_n^{a_n}$$
$$y = p_1^{b_1} \times p_2^{b_2} \times \dots p_n^{b_n}$$

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

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

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 algorithm used to determine if a number is prime.

Checking a number is prime

- Primality test is an algorithm used to determine if a number is prime.

Algorithm 2 Primality Test

Input:
Number N
Output: Prime or Not Prime

```
for i = 2 to N − 1 do
    if N is divisible by i (reminder is zero) then
        return "N is Not Prime"
    end if
end for
return "N is Prime"
```

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 $\sqrt{N}$

Algorithm 4 Primality Test

Input:
Number N
Output: Prime or Not Prime

```
for i = 2 to √N do
    if N is divisible by i (reminder is zero) then
        return "N is Not Prime"
    end if
end for
return "N is Prime"
```

Questions