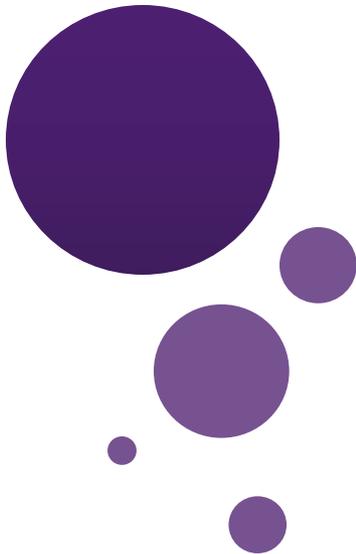




UNIVERSITY
AT ALBANY

State University of New York

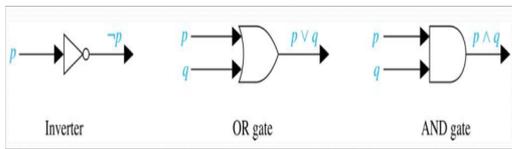


Lecture 16: Integers and Division

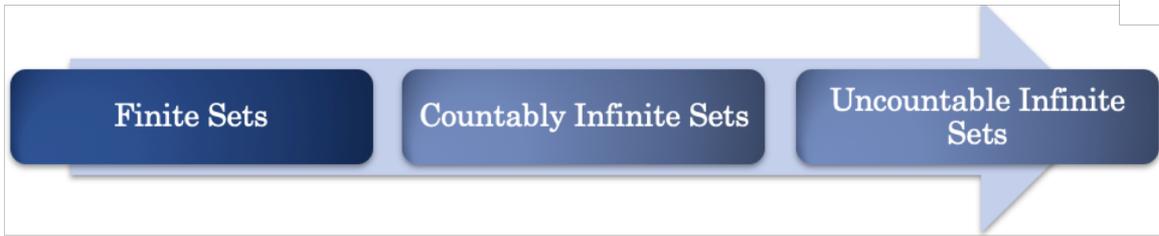
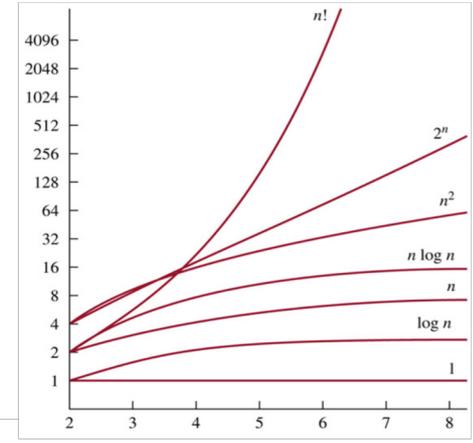
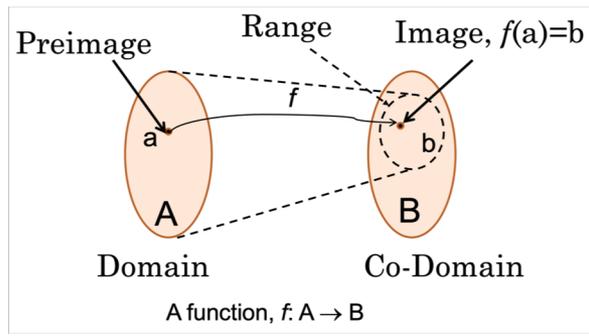
Dr. Chengjiang Long
Computer Vision Researcher at Kitware Inc.
Adjunct Professor at SUNY at Albany.
Email: clong2@albany.edu

Recap Previous Lecture

- Propositional and Logical Logic
- Rules of Inference, and Proofs
- Sets, Functions, Sequences and Matrices
- Algorithm, Growth Functions and Complexity



$$\frac{x_1 + x_2 + \dots + x_n}{n} \geq \sqrt[n]{x_1 \cdot x_2 \cdot \dots \cdot x_n}$$



Outline

- Introduction of Number Theory
- Division of Integers
- The Properties of Division
- Meaning of Integer Division

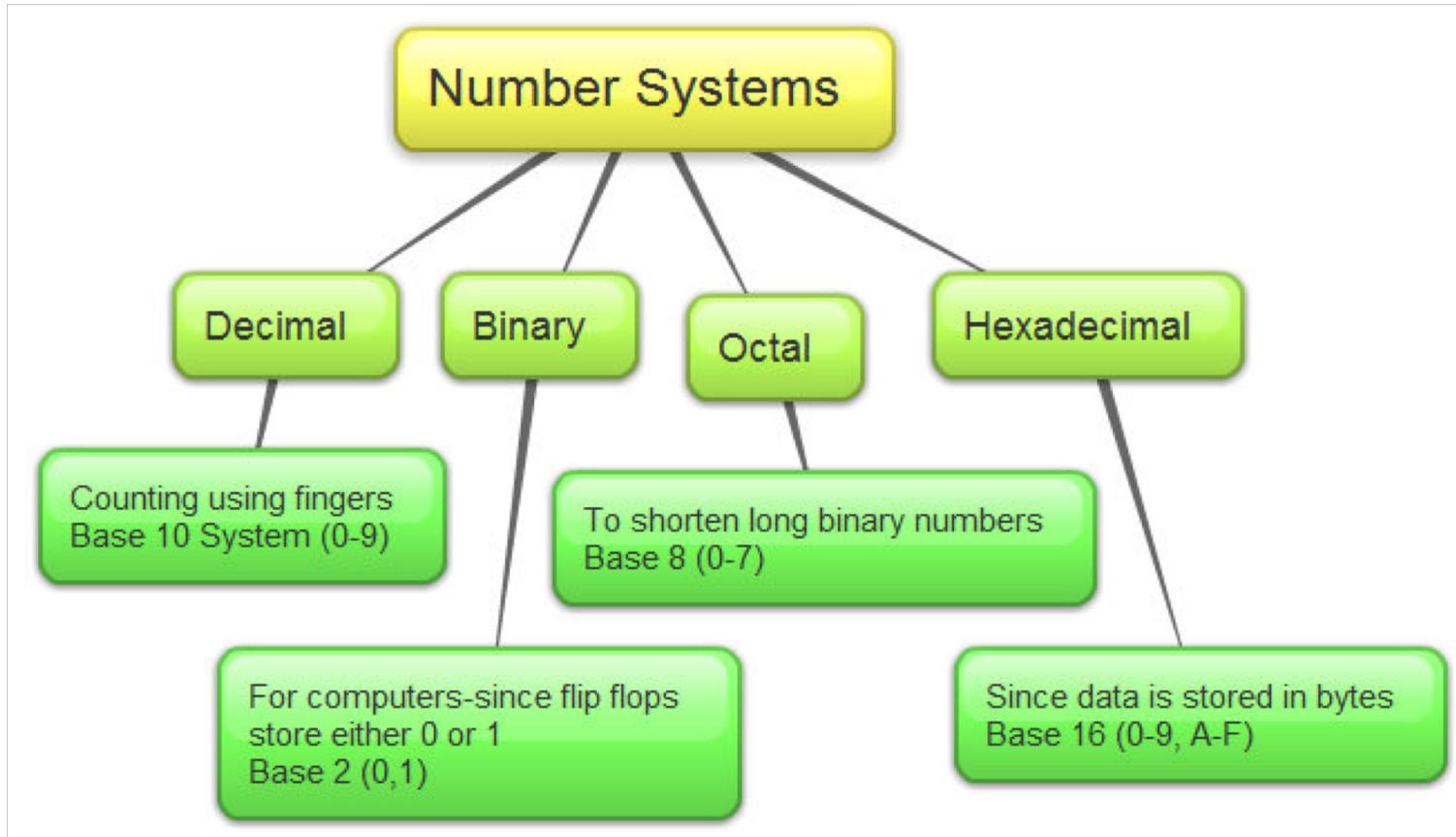
Outline

- **Introduction of Number Theory**
- Division of Integers
- The Properties of Division
- Meaning of Integer Division

Number theory

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

Representations of integers



Representations of integers

Decimal number	Binary representation	Octal representation	Hexadecimal representation
0	0	0	0
1	1	1	1
2	10	2	2
3	11	3	3
4	100	4	4
5	101	5	5
6	110	6	6
7	111	7	7
8	1000	10	8
9	1001	11	9
10	1010	12	A
11	1011	13	B
12	1100	14	C
13	1101	15	D
14	1110	16	E
15	1111	17	F
16	10000	20	10

Applications

- Number theory has many applications within computer science, including:
 - – Indexing - Storage and organization of data
 - – Encryption
 - – Error correcting codes
 - – Random numbers generators
- Key ideas in number theory include **divisibility** and the **primality** of integers.

Outline

- Introduction of Number Theory
- **Division of Integers**
- The Properties of Division
- Meaning of Integer Division

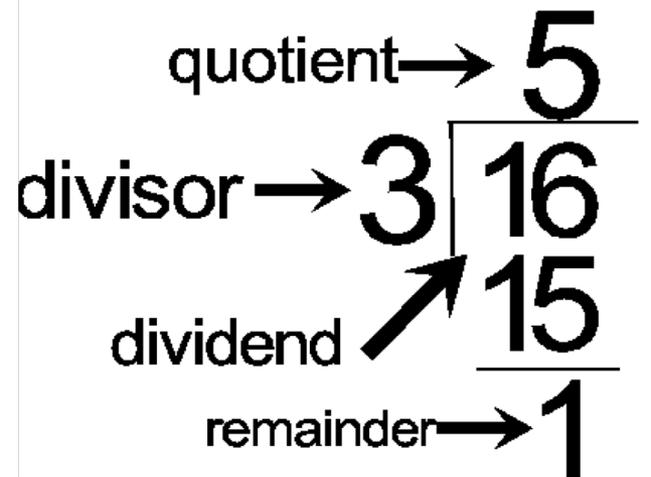
Why is division of integers so important?

Suppose that 35 friends are buying 200 tickets from you.
How to do this and keep friendship?



Division Algorithm

- If a is an integer and d is a positive integer, then there are unique integers q and r , with $0 \leq r < d$, such that $a = dq + r$.
- d is called the *divisor*.
- a is called the *dividend*.
- q is called the *quotient*.
- r is called the *remainder*.



Examples

- Read Division Algorithm carefully and answer the following questions.
- **Question:** What are the quotient and the remainder when 200 is divided by 35?
- **Answer:** The quotient is 5 and the remainder is 25.
- **Question:** What are the quotient and the remainder when -200 is divided by 35?
- **Answer:** The quotient is -6 and the remainder is 10.

Division

- **Definition:** Assume 2 integers a and b , such that $a \neq 0$ (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 **$a \mid b$** .
- If a does not divide b , we write **$a \nmid b$** .

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

Prove that if a is an integer other than 0, then

- 1 divides a .
- a divides 0.

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 ?

$$0 < kd \leq n$$

Divisibility

Question:

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

$$0 < kd \leq n$$

Answer:

Count the number of integers kd that are less than n .
What is 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 .

Outline

- Introduction of Number Theory
- Division of Integers
- **The Properties of Division**
- Meaning of Integer Division

Properties of Divisibility

Let a , b , and c be integers, where $a \neq 0$.

- (1) If $a \mid b$ and $a \mid c$, then $a \mid (b + c)$;
- (2) If $a \mid b$, then $a \mid bc$ for all integers c ;
- (3) If $a \mid b$ and $b \mid c$, then $a \mid c$.

Properties of Divisibility

Let a , b , and c be integers, where $a \neq 0$.

- (1) If $a \mid b$ and $a \mid c$, then $a \mid (b + c)$;
- (2) If $a \mid b$, then $a \mid bc$ for all integers c ;
- (3) If $a \mid b$ and $b \mid c$, then $a \mid c$.

Proof of (1): if $a \mid b$ and $a \mid c$, then $a \mid (b + c)$

- 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 $b+c$.

Properties of Divisibility

Let a , b , and c be integers, where $a \neq 0$.

- (1) If $a \mid b$ and $a \mid c$, then $a \mid (b + c)$;
- (2) If $a \mid b$, then $a \mid bc$ for all integers c ;
- (3) If $a \mid b$ and $b \mid c$, then $a \mid c$.

Proof of (2): if $a \mid b$, then $a \mid bc$ for all integers c

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

Properties of Divisibility

Let a , b , and c be integers, where $a \neq 0$.

- (1) If $a \mid b$ and $a \mid c$, then $a \mid (b + c)$;
- (2) If $a \mid b$, then $a \mid bc$ for all integers c ;
- (3) If $a \mid b$ and $b \mid c$, then $a \mid c$.

Proof of (3): if $a \mid b$ and $b \mid c$, then $a \mid c$

- If $a \mid b$, then there is some integer u such that $b = au$.
- If $b \mid c$, then there is some integer k such that $c = kb = kau = aku$, so by definition, $a \mid c$.
- Thus a divides c

Outline

- Introduction of Number Theory
- Division of Integers
- The Properties of Division
- **Meaning of Integer Division**

Meaning of Integer Division

- Understanding of division starts from natural numbers: how to represent one set as a union of several other equal sets.
- Division of natural numbers with remainder is a representing of the set as a union of other sets with equal number of elements plus one set that does not have enough elements to be equal with others.
- **Example:** 100 flowers arranged in the bunches of 12 will result in 8 bouquets and 4 flowers.

Meaning of Integer Division

- Any natural number b could be divided by any natural number a with remainder r such as
 - $b = qa + r$
- and there are three possible cases:
 - $a \mid b \rightarrow r = 0.$
 - $a > b \rightarrow q = 0, r = b.$
 - $a \nmid b \rightarrow q \in \mathbf{Z}^+, r \in \mathbf{Z}^+.$

Meaning of Integer Division, cont'd

- Meaning of the Integer Division of positive integers is covered by Integer Division of natural numbers.
- But what about negative integers divided by positive integer?
- **Example:**
- Suppose, there is a loan of \$1000 (negative number for accounting) that should be paid by 7 co-borrowers equally and rounded to \$1.
- That is $7 \times \$143 = \1001 .
- \$1 is the remainder.

Integer Division of Negative Numbers

- **Algorithm:**

1. Find absolute values (modulus) of dividend a and divisor b .
2. Divide moduli.
3. If remainder of step 2 is 0, the answer is the number opposite to the result of step 2.
4. If remainder of step 2 is not 0 then add 1 to the quotient of the result of step 2 and find the opposite to it. It is the quotient q .
5. The remainder is $r = a - b \cdot q$.

Definitions of Functions **div** and **mod**

- There are special notation to define the quotient and the remainder of Integer Division of a by d :
 - $q = a \mathbf{div} d$
 - $r = a \mathbf{mod} d$

Examples

A. Find $-17 \text{ div } 5$ and $-17 \text{ mod } 5$.

1. $|-17| = 17, |5| = 5.$

2. $17 \text{ div } 5 = 3, 17 \text{ mod } 5 = 2.$

3. $-(3 + 1) = -4. \mathbf{-17 \text{ div } 5 = -4.}$

4. $-17 - 5 \cdot (-4) = -17 - (-20) = -17 + 20 = 3. \mathbf{-17 \text{ mod } 5 = 3.}$

B. Find $-1404 \text{ div } 26$ and $-1404 \text{ mod } 26$.

Answer: $-1404 \text{ div } 26 = -54, -1404 \text{ mod } 26 = 0.$

Next class

- Topic: Modular Arithmetic
- Pre-class reading: Chap 4.1-4.2

