UNIVERSITY AT ALBANY

State University of New York

Lecture 15: Integers and Division

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

About Midterm Exam 1

University at Albany, SUNY

College of Engineering and Applied Sciences, Computer Science

ISEN/ISCI-210: Discrete Structures

Fall 2018

Midterm Exam 1

Name: ________________ ID #: ________________ Score: ________________

- This is a CLOSE BOOK & CLOSE NOTE exam. Also, you cannot access the Internet or use your laptop computer. Do the exam independently.
- Logical equivalence tables are given on Page 2.
- There are a total of 100 points in the exam. Plan your work accordingly.
- Write out the steps for all problems to receive the full credit. Use additional pages if necessary.
- Date: Oct 8th, 2018.
- Location: Lecture center hall 25.
- Time: 9:20 am - 10:20 am (can be extended to 10:35 am).

About Midterm Exam 1

Problem	Points	Scores
Problem 1: True or False	20	
Problem 2: True Table and Logical Equivalence	20	
Problem 3: Predicatives and Quantifiers	20	
Problem 4: Set, Sequences and Summation	20	
Problem 5: Functions	20	

About Midterm Exam 1

Figure 1: Logical equivalences.

Equivalence	*Name*
$p \wedge \mathbf{T} \equiv p$ $p \vee \mathbf{F} \equiv p$	Identity laws
$p \vee \mathbf{T} \equiv \mathbf{T}$ $p \wedge \mathbf{F} \equiv \mathbf{F}$	Domination laws
$p \vee p \equiv p$ $p \wedge p \equiv p$	Idempotent laws
$\neg(\neg p) \equiv p$	Double negation law
$p \vee q \equiv q \vee p$ $p \wedge q \equiv q \wedge p$	Commutative laws
$(p \vee q) \vee r \equiv p \vee (q \vee r)$ $(p \wedge q) \wedge r \equiv p \wedge (q \wedge r)$	Associative laws
$p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$ $p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$	Distributive laws
$\neg(p \wedge q) \equiv \neg p \vee \neg q$ $\neg(p \vee q) \equiv \neg p \wedge \neg q$	De Morgan's laws
$p \vee (p \wedge q) \equiv p$ $p \wedge (p \vee q) \equiv p$	Absorption laws
$p \vee \neg p \equiv \mathbf{T}$ $p \wedge \neg p \equiv \mathbf{F}$	Negation laws

$$p \rightarrow q \equiv \neg p \vee q$$
$$p \rightarrow q \equiv \neg q \rightarrow \neg p$$
$$p \vee q \equiv \neg p \rightarrow q$$
$$p \wedge q \equiv \neg(p \rightarrow \neg q)$$
$$\neg(p \rightarrow q) \equiv p \wedge \neg q$$
$$(p \rightarrow q) \wedge (p \rightarrow r) \equiv p \rightarrow (q \wedge r)$$
$$(p \rightarrow r) \wedge (q \rightarrow r) \equiv (p \vee q) \rightarrow r$$
$$(p \rightarrow q) \vee (p \rightarrow r) \equiv p \rightarrow (q \vee r)$$
$$(p \rightarrow r) \vee (q \rightarrow r) \equiv (p \wedge q) \rightarrow r$$

(a) Involving conditional statements.

$$p \leftrightarrow q \equiv (p \rightarrow q) \wedge (q \rightarrow p)$$
$$p \leftrightarrow q \equiv \neg p \leftrightarrow \neg q$$
$$p \leftrightarrow q \equiv (p \wedge q) \vee (\neg p \wedge \neg q)$$
$$\neg(p \leftrightarrow q) \equiv p \leftrightarrow \neg q$$

(b) Involving biconditional statements.

Outline

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

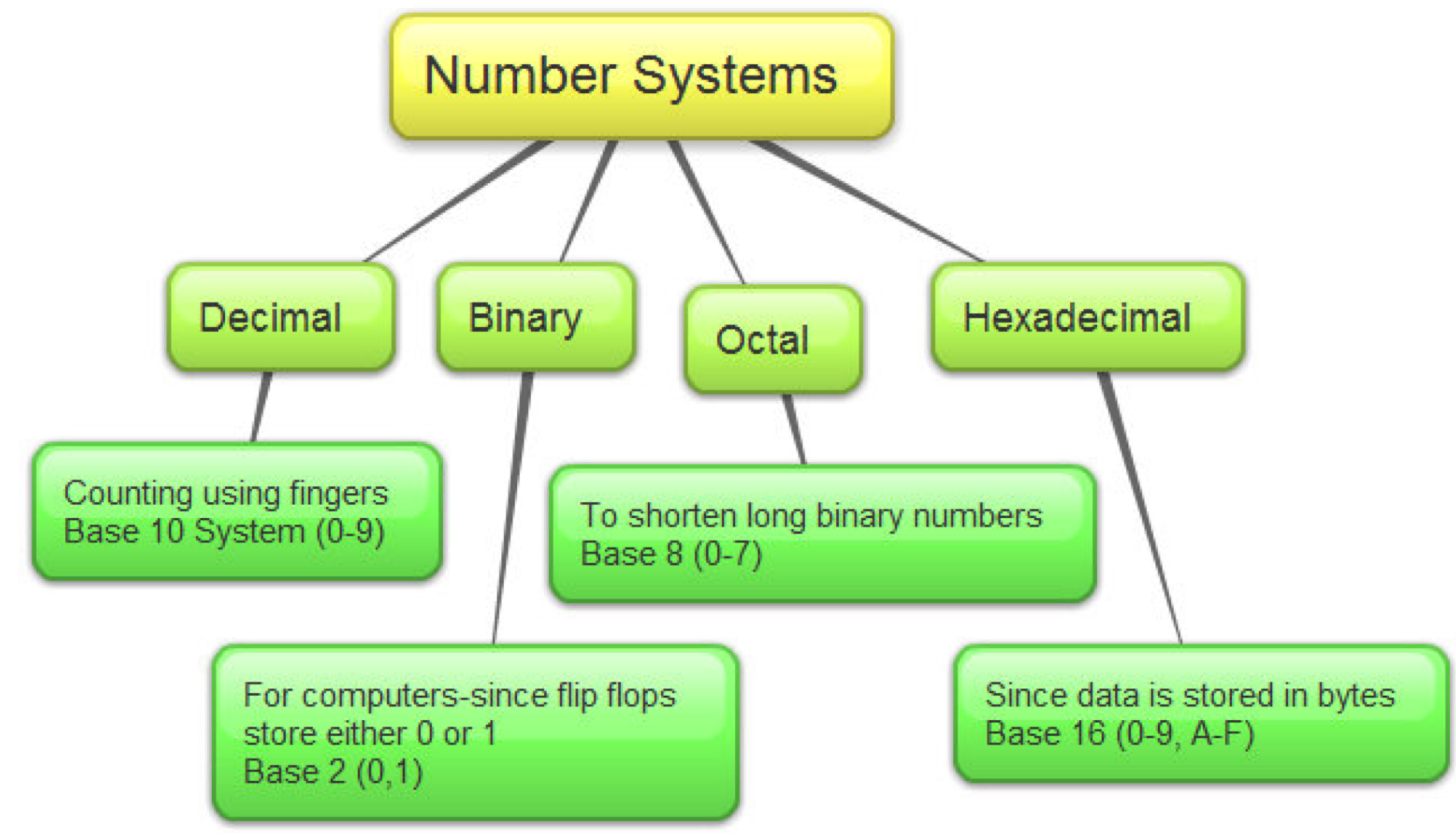
Outline

- **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:
  - – Z integers {…, -2,-1, 0, 1, 2, …}
  - – Z+ positive integers {1, 2, …}

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

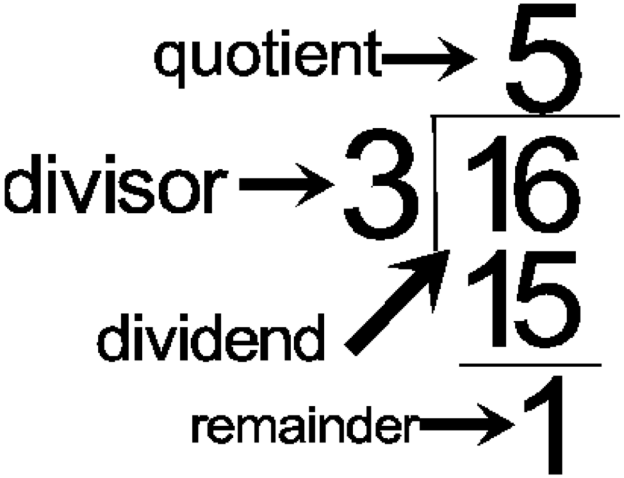
- Introduction of Number Theory
- **Division of Integers**
- The Properties of Division
- Meaning of Integer Division

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 | b**.
- If *a* does not divide *b*, we write $a \nmid b$.

Examples

$4 \mid 24$ True or False ?

True

- 4 is a factor of 24
- 24 is a multiple of 4

$3 \mid 7$ 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 $0 < kd \leq n$?

$0 < kd \leq n$ --> $0 < k \leq n/d$ 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 | 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.

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 | 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

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 | b and b | c, then a | c

- If a | b, then there is some integer u such that b = au.
- If b | c, then there is some integer k such that c = kb = kau=aku, so by definition, a | 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 7x$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*:
  - $q = a$ **div** d
  - $r = a$ **mod** d

Examples

A. Find −17 div 5 and − 17 mod 5.

1. | −17 | = 17, | 5 | = 5.
2. 17 div 5 = 3, 17 mod 5 = 2.
3. −(3 + 1) = − 4. **− 17 div 5 = −4**.
4. −17−5·(−4) = −17 − (−20) = − 17 + 20 = 3. **− 17 mod 5 = 3**.

B. Find −1404 div 26 and −1404 mod 26.

Answer: −1404 div 26 = − 54, −1404 mod 26 = 0.

Next class

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