

Lecture 20: Integer Representations and Algorithms

Jingjin Yu | Computer Science @ Rutgers

Outline

Copyrighted Material – Do Not Distribute

- ▶ Lecture 19 review
- ▶ Base b representation
 - ▷ From decimal to base b
 - ▷ From base b to decimal
 - ▷ Between binary, octal, and hexadecimal
- ▶ Binary computations
 - ▷ Addition and subtraction
 - ▷ Multiplication and division
- ▶ Modular exponentiation
- ▶ A repeating note: **make sure you read the textbook**

L19: Number Theory & Divisibility

Copyrighted Material – Do Not Distribute

- ▶ A key goal of Lecture 19 is to build up to **Theorem 5** and **Corollary 6**, which are really “**algorithms**” for helping with computation of modular arithmetic.
- ▶ **Defⁿ: Number theory** is the part of mathematics devoted to the study of integers.
- ▶ **Defⁿ: Divisibility.** Let a and b be integers. Then, a **divides** b if $b = ac$ for some integer c . Otherwise, a does not divide b .
 - ▷ Notation: a divides b : $a \mid b$, a does not divide b : $a \nmid b$
 - ▷ If $a \nmid b$, $b = aq + r$ for some integers q (**quotient**) and $0 < r < b$ (**remainder**)
- ▶ **Ex:** $a = 4, b = 12$. $a \mid b$?
- ▶ **Ex:** $a = 3, b = 10$. $a \mid b$?

L19: Properties on Divisibility

Copyrighted Material – Do Not Distribute

- ▶ **Theorem 1.** a, b , and c are integers and $a \neq 0$. Then:
 - ▷ (i) If $a | b$ and $a | c$, then $a | (b + c)$.
 - ▷ (ii) If $a | b$, then $a | bc$ for all integers c .
 - ▷ (iii) If $a | b$ and $b | c$, then $a | c$.
- ▶ **Theorem 2.** a and $d > 0$ are integers. Then there are **unique** integers q and r with $0 \leq r < d$ s.t. $a = dq + r$.
- ▶ **Ex:** $a = 47, d = 8$.
- ▶ **Ex:** $a = -14, d = 5$.

L19: Modular Arithmetic

Copyrighted Material – Do Not Distribute

- ▶ Notation: $\underline{a} \text{ mod } \underline{m}$ is the remainder of \underline{a} divided by \underline{m} .
- ▶ **Defⁿ:** Let a and b be integers and m a positive integer. We say a is congruent to b modulo m if $m \mid (a - b)$.
 - ▷ Notations:
 - $a \equiv b \pmod{m}$ if and only if $m \mid (a - b)$
 - $a \not\equiv b \pmod{m}$ if and only if $m \nmid (a - b)$
- ▶ **Theorem 3.** a, b , and $m > 0$ are integers. Then $a \equiv b \pmod{m}$ if and only if $a \text{ mod } m = b \text{ mod } m$
- ▶ **Ex:** $a = 17, b = 5, m = 6$. $a \equiv b \pmod{m}$?
- ▶ **Ex:** $a = 24, b = 516, m = 6$. $a \equiv b \pmod{m}$?

L19: More Properties

Copyrighted Material – Do Not Distribute

- ▶ **Theorem 4.** $a \equiv b \pmod{m}$ if and only if $a = b + km$ for some integer k .
- ▶ **Theorem 5.** $m > 0$ is an integer. If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$ then $a + c \equiv b + d \pmod{m}$ and $ac \equiv bd \pmod{m}$.
- ▶ **Ex:** $m = 7, a = 11, b = 18, c = 22, d = 8$
- ▶ **Corollary 6.** a, b and $m > 0$ are integers. Then
 - ▷ $(a + b) \bmod m = ((a \bmod m) + (b \bmod m)) \bmod m.$
 - ▷ $(ab) \bmod m = ((a \bmod m)(b \bmod m)) \bmod m.$
- ▶ **Ex:** $a = 13241, b = 479, m = 3.$
 - ▷ $(a + b) \bmod m = ?$
 - ▷ $(ab) \bmod m = ?$



Representing Integers

Copyrighted Material – Do Not Distribute

- ▶ For everyday: decimals are **base 10** representations.

89546 2222

- ▶ Why do we use decimal numbers?
- ▶ Mayans use base 20 and base 5
- ▶ We can use any positive integer as the base
 - ▶ Base 1: unary numbers, e.g., $(1111111)_1$
 - ▶ Base 2: binary numbers, e.g., $(0010\ 1110)_2$
 - ▶ Base 3: ternary
 - ▶ Base 8: octal
 - ▶ Base 16: hexadecimal

0	1	2	3	4
•	•	••	•••	••••
5	6	7	8	9
—	—	—	—	—
10	11	12	13	14
—	—	—	—	—
15	16	17	18	19
—	—	—	—	—
20	21	22	23	24
•	•	•	•	•
—	—	—	—	—
25	26	27	28	29
•	•	•	•	•
—	—	—	—	—
30	31	32	33	34
•	•	•	•	•
—	—	—	—	—
35	36	37	38	39
•	•	•	•	•
—	—	—	—	—
40	41	42	43	44
••	••	••	••	••
—	—	—	—	—
45	46	47	48	49
••	••	••	••	••
—	—	—	—	—

Representing a Number in Base b

Copyrighted Material – Do Not Distribute
Base b to ~~base 10~~ ~~base 10~~

- ▶ Breaking down a number: $28 = 2 \times 10^1 + 8 \times 10^0$
- ▶ Ex: Represent $(28)_{10}$ in binary (base 2)

$$28 = 16 + 8 + 4$$
$$\begin{array}{r} 2^4 \\ 2^3 \\ 2^2 \\ 2^1 \\ 2^0 \end{array} = \begin{array}{r} 4 \\ 3 \\ 2 \\ 1 \\ 0 \end{array} = (1110)_2$$

- ▶ Ex: Represent $(28)_{10}$ in octal (base 8)

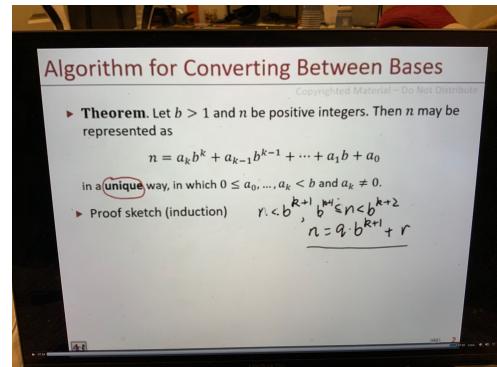
11:20 AM Sat Nov 28 Back CS 205 SEC 01-02-03

Representing a Number in Base b

Copyrighted Material – Do Not Distribute

- ▶ Breaking down a number: $28 = 2 \times 10^1 + 8 \times 10^0$
- ▶ Ex: Represent $(28)_{10}$ in binary (base 2)
 $28 = 16 + 8 + 4 = (1110)_2$
- ▶ Ex: Represent $(28)_{10}$ in octal (base 8)
 $28 = 3 \times 8^1 + 4 \times 8^0 = (34)_8$

HC Speed Scrubbing
Slide your finger up to adjust the scrubbing rate.



Algorithm for Converting Between Bases

Copyrighted Material – Do Not Distribute

- ▶ **Theorem.** Let $b > 1$ and n be positive integers. Then n may be represented as

$$n = a_k b^k + a_{k-1} b^{k-1} + \cdots + a_1 b + a_0$$

in a **unique** way, in which $0 \leq a_0, \dots, a_k < b$ and $a_k \neq 0$.

- ▶ Proof sketch (induction)

Convert from Base b to Base 10

Copyrighted Material – Do Not Distribute

- ▶ **Algorithm** for converting from base b to base 10: simply compute the polynomial!

- ▶ **Ex:** $(101011111)_2$ to base 10

$$\begin{array}{r} (7016)_8 \\ 8^7 8^6 8^5 8^4 8^3 8^2 8^1 8^0 \\ 2^8 + 2^6 + 2^4 + 2^3 + 2^2 + 2^1 + 2^0 = 23 \end{array}$$

- ▶ **Ex:** $(7016)_8$ to base 10

$$7 \times 8^3 + 1 \times 8^1 + 6 = 3598$$

$$16^0 \times 16^4 + 16 \times 16^3 + 16^2 \times 16^1$$

- ▶ **Ex:** $(A7E)_{16}$ to base 10

$$A \times 16^2 + 7 \times 16^1 + E \times 16^0 = 2686$$

Convert from Base 10 to Base b

$$\begin{array}{r} 12345 \\ \times 8 = 1543 \quad R_1 \\ 1543 \\ \times 8 = 192 \quad R_2 \\ 192 \\ \times 8 = 24 \quad R_3 \\ 24 \\ \times 8 = 3 \quad R_4 \\ 3 \\ = 0 \quad R_5 \end{array}$$

Copyrighted Material – Do Not Distribute

- ▶ **Algorithm** for converting from base 10 to base b : Given n , $n = n_0 b + r_0$ for some $0 \leq r_0 < b$, r_0 is the last digit. Then, repeat the same with n_0 to obtain $n_0 = n_1 b + r_1$, until we reach $n_k = 0$. The base b number is $(r_k \dots r_0)_b$

- ▶ Ex: Convert 12345 to octal.

- ▶ Ex: Convert 37 to binary.

$$37 \rightarrow 2 \times 18 + 1 \rightarrow r_0$$

$$18 \rightarrow 2 \times 9 + 0 \rightarrow r_1$$

$$9 \rightarrow 2 \times 4 + 1 \rightarrow r_2$$

$$4 \rightarrow 2 \times 2 + 0 \rightarrow r_3$$

$$2 \rightarrow 2 \times 1 + 0 \rightarrow r_4$$

$$1 \rightarrow 2 \times 0 + 1 \rightarrow r_5$$

$$\begin{array}{r} 12345 = 1543 \times 8 + 3 \rightarrow r_0 \\ 1543 = 192 \times 8 + 7 \rightarrow r_1 \\ 192 = 24 \times 8 + 0 \rightarrow r_2 \\ 24 = 3 \times 8 + 0 \rightarrow r_3 \\ 3 = 0 \times 8 + 3 \rightarrow r_4 \end{array}$$

$$(100101)_2$$

Convert between Binary, Octal, Hexadecimal

Copyrighted Material – Do Not Distribute

- Ex: Convert ~~(110 0011)₂~~ to octal.

143

$$2^6 + 2^5 + 2^1 + 2^0 = 99$$

$$99 = 12 \times 8 + 3 \quad 12 \times 8 + 1 = 0 \times 8 + 1 \quad (143)_8$$
$$(1 \overline{)} \frac{100}{4} (01)_2 = (143)_8$$

- Ex: Convert $(56)_8$ to binary.

$$\begin{array}{r} 100 \\ 56 \end{array} \rightarrow (101 \quad 110)_2$$

- Ex: Convert $(1110 \ 1011)_2$ to hexadecimal and back.

$$\begin{array}{r} 1110 \ 1011 \\ 764 \ 3210 \\ \hline 2486 \end{array} \quad \overbrace{\quad}^E \quad \overbrace{\quad}^B \quad (BB)_{16}$$

$$\rightarrow (110 \ 1011)_2$$

Binary Addition and Subtraction

Copyrighted Material – Do Not Distribute

- Ex: $1110_2 + 1011_2$

The image shows a hand-drawn mathematical expression within a large, irregular oval frame. The expression consists of two sets of parentheses: a pair of outer parentheses enclosing a pair of inner parentheses. Inside the inner parentheses, there is a single digit '1' followed by a circled '0'. The entire drawing is done in black ink on a white background.

$$\begin{array}{r}
 & \text{Copyr} \\
 & | \quad | \quad | \quad | \quad 0 \\
 + & | 0 \quad 1 \quad) \\
 \hline
 & | \quad 0 \quad 0 \quad)
 \end{array}$$

- $$\begin{array}{r} 1011 \\ + 101 \\ \hline 1010 \end{array}$$

$$\begin{array}{r}
 \begin{array}{c} (01) \\ + 011 \\ \hline 100 \end{array} & \left(\begin{array}{c} 110 \\ - 10 \\ \hline 100 \end{array} \right) = \underline{101} \\
 & \begin{array}{c} 101 \\ - 10 \\ \hline 100 \end{array} \end{array}$$

$$101 \rightarrow 0|0 \xrightarrow{\text{skip}} \textcircled{0}|0|0 \quad \text{add 1 for negative}$$

1011
1101
16 5161

Binary Addition and Subtraction

► Ex: $1110_2 + 1011_2$

$$\begin{array}{r} 1110 \\ + 1011 \\ \hline 1000 \end{array}$$

► Ex: $1011_2 - 101_2$

$$\begin{array}{r} 1011 \\ - 101 \\ \hline 0110 \end{array}$$

$$(110)_2$$

Copyrighted Material — Do Not Distribute

Ex

$$(101)_2 - (100)_2$$

$$\boxed{110}$$

$$1011$$

$$\begin{array}{r} 010 \\ + 1011 \\ \hline 1110 \end{array}$$

$$2011$$

$$\begin{array}{r} 010 \\ + 1000 \\ \hline 1010 \end{array}$$

$$1100$$

$$\boxed{110}$$

Binary Multiplication and Division/Mod

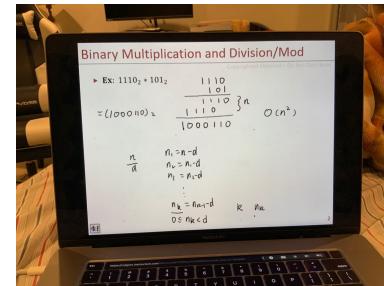
Copyrighted Material – Do Not Distribute

► Ex: $1110_2 * 101_2$

$$\begin{array}{r} 1110 \\ \times 101 \\ \hline 0000 \\ 1110 \\ + 0000 \\ \hline 10110 \end{array}$$

$$\begin{array}{r} 1110 \\ \times 101 \\ \hline 1110 \\ + 1110 \\ \hline 10110 \end{array}$$

$$10110$$



Modular Exponentiation

1026 mod 7 = 4

Copyrighted Material – Do Not Distribute

- Ex: $5^{11} \text{ mod } 7$

