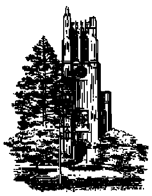
Monday June 13, 2016
Lecture 16

Number Theory



456

Notables

- Reach Chapter 4
- Homework #9
  - Page 229, Problems 2, and 16
  - Page 244, Problems 6, 10, and 14,
  - Page 245, Problems 28, and 32
    - Due, Tuesday June 14, 2016

457

Homework 10; Due Thursday June 16

1. Using the method discussed in class, convert (long hand)
   a. Decimal (that is, base 10) 8888 to binary
   b. Decimal 2555 to base 6
   c. Decimal 8990 to base 19; use symbols 0-9 and A-Z
   You must show ALL your steps to receive full credit.
2. Convert $(260.260)_9$ to base 10.
3. Carry out the following additions in the given base:
   a. $(5665)_7 + (4664)_7 = (\quad\quad)_7$
   b. $(AB56)_{16} + (9868)_{16} = (\quad\quad)_{16}$
4. Page 255, Problem 26
5. Page 256, Problem 30(d), and Problem 48(d)
6. Page 272, Problem 4(f), 21(c), 24(b), and 40(e)

458

Modular Arithmetic

- Recall that the *mod* function is a mapping:
  $mod : \mathbf{Z} \times \mathbf{Z}^+ \rightarrow \mathbf{N}$ where
  $$n \text{ mod } m = n - m \times \lfloor n/m \rfloor$$
- Examples:

  5 mod 3 = $5 - (3 \times \lfloor 5/3 \rfloor) = 5 - (3 \times \lfloor 1.6 \rfloor) = 5 - (3 \times 1) = 2$

- Alternatively,
  f_m: $\mathbf{Z} \rightarrow \{0, 1, 2, \ldots, m-1\}$, where
  $f_m(n) = n$ mod m
  - Note that f_m is onto, but not one-to-one.

459

Congruence

- Definition: Suppose a and b are integers, and m is a *positive* integer. If the following equality
  $$a \text{ mod } m = b \text{ mod } m$$
  holds then we say that a is *congruent* to b *modulo* m, and we donate it by $a \equiv b \pmod{m}$.
  - 12 mod 5 = 2
  - 17 mod 5 = 2
    - Then $12 \equiv 17 \pmod 5$
- Alternative definition: $a \equiv b \pmod{m}$ if and only if
  $$m \mid (a - b)$$

460

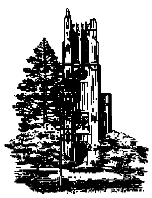
Congruence…

- Theorem: $\forall m \in Z^+\ \forall a \in Z\ \forall b \in Z$
  $a \equiv b \pmod{m} \iff \exists k \in Z\ a = b + km$
- Theorem: If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then:
  - $a + c \equiv b + d \pmod{m}$, and
  - $ac \equiv bd \pmod{m}$.

461

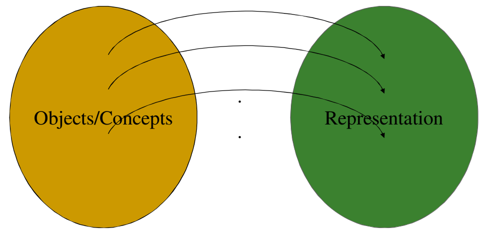
Integers & Algorithms

Section 4.2



462

Object Representation



A one-to-one function is required

463

Object Representation…

- Need symbols; how many?
- What are other issues?
  - Physical cost of representation
  - Representation and algorithms
- We'll concentrate on "number" representation.

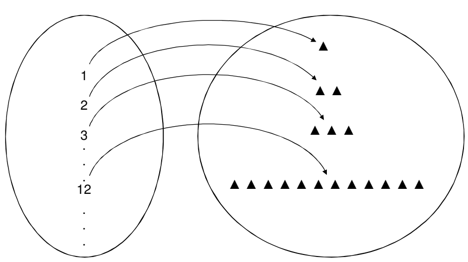
464

Issues in Representation

- Cost (how to define?)
  - How many symbols
  - Operations
  - Recovery
  - Transmission (another representation)
- For counting, how many symbols do we need?

465

Example: Using only one symbol



As long as we have a one-to-one function, we have a correct presentation

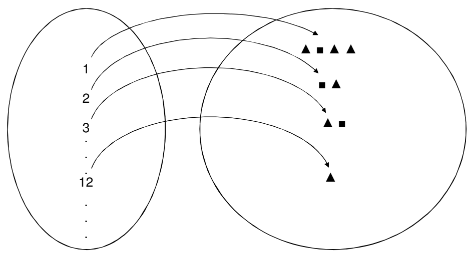
466

Understanding Number Encoding

- Suppose we have the following "symbol"
  - ▲
- How would you encode "numbers"?
  - We may have to employ a "manual" or a "translation table"
- Suppose now that we have the following symbols
  - ▲ and ■
- How would you encode "numbers" now?

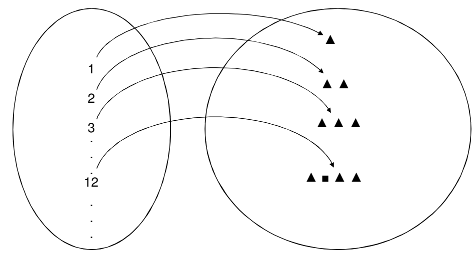
467

Example: Using two symbols



As long as we have a one-to-one function, we have a correct presentation

Example: Using two symbols



As long as we have a one-to-one function, we have a correct presentation

Understanding Number Representation

- We usually use {0, 1, 2, 3, 4, 5, 6, 7, 8, 9} as *base* to write numbers, but we can use any *base*.
- Remember that :

$$453 = 4 \cdot 10^2 + 5 \cdot 10^1 + 3 \cdot 10^0$$

- The above is a *positional system* representation
- It has a "compact" manual
- There are other representations

Representation of Integers…

- Theorem: Let b be a positive integer > 1. We can write every positive integer *uniquely* in the following form:

$$n = a_k b^k + a_{k-1} b^{k-1} + \cdots + a_1 b^1 + a_0 b^0$$

where k is a positive integer and
$a_0, a_1, \ldots, a_k \in \{0, 1, 2, \ldots, b-1\}$ and $a_k \neq 0$.

- Example:

$$453 = 4 \cdot 10^2 + 5 \cdot 10^1 + 3 \cdot 10^0$$

$$n = a_2 b^2 + a_1 b^1 + a_0 b^0$$

Base conversion

- To convert a number, say 6543, in base 10 to an equivalent number in another base, say 7, we need to come up with the coefficients in the following expression:

$$6543 = a_4 7^4 + a_3 7^3 + a_2 7^2 + a_1 7^1 + a_0 7^0$$

- It seems that we have only one equation but many unknowns.
  - We use the restriction that the coefficients are all integers between 0 and 6.
- A series of divisions would do

Example: Base conversion

$$6543 = a_4 7^4 + a_3 7^3 + a_2 7^2 + a_1 7^1 + a_0 7^0$$

$$6543 = a_4 7^4 + a_3 7^3 + a_2 7^2 + a_1 7^1 + a_0$$

$$6543 = \underbrace{(a_4 7^3 + a_3 7^2 + a_2 7 + a_1)}_{Quotient} 7 + \underbrace{a_0}_{Remainder}$$

$$6543 = 934 \times 7 + 5$$

$$934 = a_4 7^3 + a_3 7^2 + a_2 7 + a_1$$

$$934 = (a_4 7^2 + a_3 7 + a_2) 7 + a_1$$

and so on...

Integer n and base b

$$n = a_k b^k + a_{k-1} b^{k-1} + \cdots + a_3 b^3 + a_2 b^2 + a_1 b^1 + a_0 b^0$$

$$n = (a_k b^{k-1} + a_{k-1} b^{k-2} + \cdots + a_3 b^2 + a_2 b^1 + a_1) b \ + a_0$$

$$n = ((a_k b^{k-2} + a_{k-1} b^{k-3} + \cdots + a_3 b^1 + a_2) b \ + a_1) b \ + a_0$$

Algorithm example

- Step 1: *Take* two positive integers n and b.
- Step 2: *Divide* n by b, and let q and r be the quotient and the remainder, respectively.
- Step 3: *print* r
- Step 4: *if* q is zero, *stop*.
- Step 5: *treat* q as n and *go to* step 2.

From *decimal* (base 10) to another base

n is to be converted

b is desired new base

a_k is kth digit of number

(k goes from right to left)

The base b expansion of n is

$$(a_{k\text{-}1} \ldots a_1 a_0)_b$$

$q = n$
$k = 0$
while ($q \neq 0$)
  $a_k \leftarrow q \bmod b$
  $q \leftarrow \left\lfloor \frac{q}{b} \right\rfloor$
  $k \leftarrow k+1$
end while

Example: Decimal 50 to base 2

$50 = 25*2 + 0$

$25 = 12*2 + 1$

$12 = 6*2 + 0$

$6 = 3*2 + 0$

$3 = 1*2 + 1$

$1 = 0*2 + 1$

So, the base 2 representation is 110010

Exercise:

- Decimal 229 to base 8
  - $229 = 28*8 + 5$
  - $28 = 3*8 + 4$
  - $3 = 0*8 + 3$
- So, decimal 229 = $(345)_8$
- Convert $(345)_6$ to base 10
  - $345 = 5\times6^0 + 4\times6^1 + 3\times6^2 = 137$

Exercise:

- Decimal 7996 to base 25
  - $7996 = 319 * 25 + L$
  - $319 = 12 * 25 + J$
  - $12 = 0 * 25 + C$

  - Number 7996 in decimal has CJL representation in base 25

Converting 0.875 to binary

$0.875 = 8 \times 10^{-1} + 7 \times 10^{-2} + 5 \times 10^{-3}$

Converting to base 2 means we want

$0.875 = a_1 \times 2^{-1} + a_2 \times 2^{-2} + a_3 \times 2^{-3} + a_4 \times 2^{-4} + \cdots$

So we need to find the a_i. Note that

$2 \times 0.875 = 1.75 = a_1 + a_2 \times 2^{-1} + a_3 \times 2^{-2} + a_4 \times 2^{-3} + \cdots$

Thus $a_1 = 1$. Repeating the same idea, we get

$2 \times 0.75 = 1.5 \Rightarrow a_2 = 1$

$2 \times 0.5 = 1.0 \Rightarrow a_3 = 1$

Thus $0.875 = (0.111)_2$

480

Exercise

- Represent $(0.1)_{10}$ in binary
  - 2 × 0.1 = 0.2
  - 2 × 0.2 = 0.4
  - 2 × 0.4 = 0.8
  - 2 × 0.8 = 1.6
  - 2 × 0.6 = 1.2
  - 2 × 0.2 = 0.4
  - 2 × 0.4 = 0.8
  - 2 × 0.8 = 1.6
  - 2 × 0.6 = 1.2
  - …… $(0.1)_{10}$ is $(0.000110011……)_2$

481

Exercise

- Convert 6.96 to binary, up to 5 places
  - First we convert 6 to binary, which is 110
  - 0.96 ×2 = 1.92, so the first digit after binary point is 1
  - 0.92 ×2 = 1.84, so the 2nd digit after binary point is 1
  - 0.84 ×2 = 1.68, so 3rd digit after binary point is 1
  - 0.68 ×2 = 1.36, so the 4th digit after binary point is 1
  - 0.36 ×2 = 0.72, so the 5th digit after binary point is 0
  - ….
  - So, 6.96 is 110.11110…. in binary

482