CS 441 Discrete Mathematics for CS
Lecture 14

Integers: applications, base conversions.

Milos Hauskrecht
milos@cs.pitt.edu
5329 Sennott Square

Modular arithmetic in CS

Modular arithmetic and congruencies are used in CS:

- **Pseudorandom number generators**
- **Hash functions**
- **Cryptology**

Pseudorandom number generators

- **Some problems we want to program need to simulate a random choice.**
- **Examples: flip of a coin, roll of a dice**

We need a way to generate random outcomes

Basic problem:

- assume outcomes: 0, 1, .. N
- generate the random sequences of outcomes

- Pseudorandom number generators let us generate sequences that look random
- **Next:** linear congruential method

Pseudorandom number generators

Linear congruential method

- We choose 4 numbers:
  - the modulus m,
  - multiplier a,
  - increment c, and
  - seed x_0,

  such that 2 =< a < m, 0 =< c < m, 0 =< x_0 < m.

- We generate a sequence of numbers $x_1, x_2\ x_3 \dots x_n \dots$ such that 0 =< x_n < m for all *n* by successively using the congruence:
  - $\mathbf{x_{n+1} = (a.x_n + c) \bmod m}$

Pseudorandom number generators

Linear congruential method:

- $x_{n+1} = (a.x_n + c) \bmod m$

Example:

- Assume : m=9,a=7,c=4, $x_0 = 3$

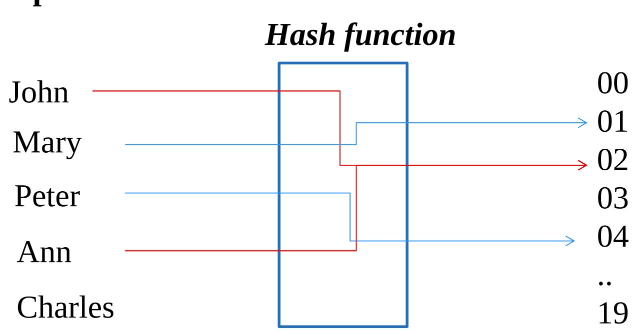
- x_1= 7*3+4 mod 9=25 mod 9 =7
- x_2 = 53 mod 9 = 8
- x_3 = 60 mod 9 = 6
- x_4= 46 mod 9 =1
- x_5 = 11 mod 9 =2
- x_6 = 18 mod 9 =0
- ....

Hash functions

A ***hash function*** is an algorithm that maps data of arbitrary length to data of a fixed length.

The values returned by a hash function are called **hash values** or **hash codes.**

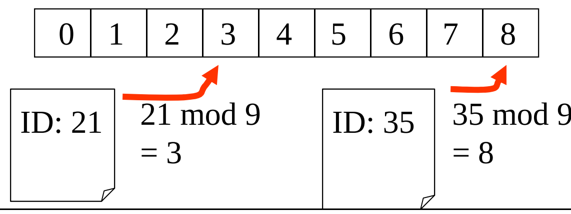
Example:



Hash functions

- **Problem:** Given a large collection of records, how can we store and find a record quickly?
- **Solution:** Use a hash function calculate the location of the record based on the record's ID.
- **Example:** A common hash function is
  - $h(k) = k \textbf{ mod } n$,

  where n is the number of available storage locations.



Hash function

An example of a hash function that maps integers (including very large ones) to a subset of integers 0, 1, .. m-1 is:

h(k) = k mod m

Example: Assume we have a database of employes, each with a unique ID – a social security number that consists of 8 digits. We want to store the records in a smaller table with m entries. Using h(k) function we can map a social secutity number in the database of employes to indexes in the table.

Assume: h(k) = k mod 111

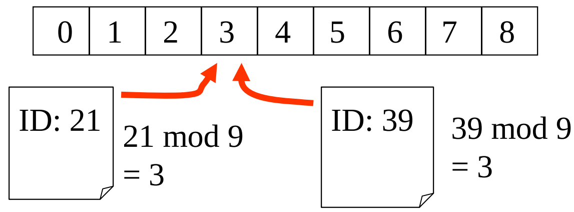
Then:

h(064212848) = 064212848 mod 111 = 14

h(037149212) = 037149212 mod 111 = 65

Hash functions

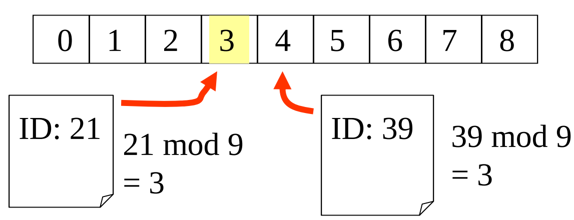
- **Problem:** two documents mapped to the same location



Hash functions

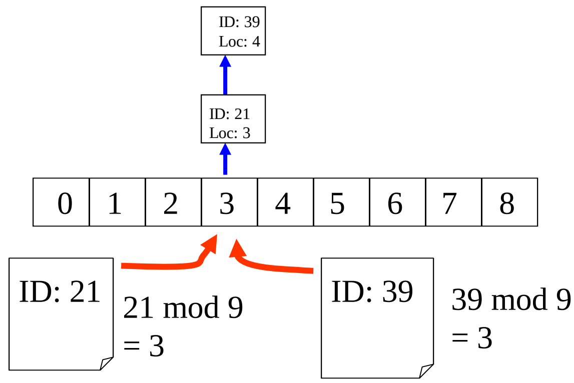
- **Solution 1:** move the next available location
  - Method is represented by a sequence of hash functions to try

$$h_0(k) = k \textbf{ mod } n$$
$$h_1(k) = (k+1) \textbf{ mod } n$$
$$\ldots$$
$$h_m(k) = (k+m) \textbf{ mod } n$$



Hash functions

- **Solution 2:** remember the exact location in a secondary structure that is searched sequentially



M. Hauskrecht

Cryptology

Encryption of messages.

- **Ceasar cipher:**
- Shift letters in the message by 3, last three letters mapped to the first 3 letters, e.g. A is shifted to D, X is shifted to A

How to represent the idea of a shift by 3?

- There are 26 letters in the alphabet. Assign each of them a number from 0,1, 2, 3, .. 25 according to the alphabetical order.

A B C D E F G H I J K L M N O P Q R S T U Y V X W Z

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

- The encryption of the letter with an index p is represented as:
    - $f(p) = (p + 3) \bmod 26$

M. Hauskrecht

Cryptology

Encryption of messages using a shift by 3.

- The encryption of the letter with an index p is represented as:
  - f(p) = (p + 3) mod 26

Coding of letters:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	Y	V	X	W	Z
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

- **Encrypt message:**
  - **I LIKE DISCRETE MATH**
  -

Cryptology

Encryption of messages using a shift by 3.

- The encryption of the letter with an index p is represented as:
  - f(p) = (p + 3) mod 26

Coding of letters:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	Y	V	X	W	Z
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

- **Encrypt message:**
  - **I LIKE DISCRETE MATH**
  - **L 0LNH GLYFUHVH PDVK.**

Cryptology

How to decode the message ?

- The encryption of the letter with an index p is represented as:
  - $f(p) = (p + 3) \bmod 26$

Coding of letters:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	Y	V	X	W	Z
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

- **What method would you use to decode the message:**
  - $\mathbf{f^{-1}(p) = (p-3) \bmod 26}$

Representations of Integers

- In the modern world, we use *decimal,* or *base* 10, *notation* to represent integers. For example when we write 965, we mean $9 \cdot 10^2 + 6 \cdot 10^1 + 5 \cdot 10^0$.
- We can represent numbers using any base b, where b is a positive integer greater than 1.
- The bases $b = 2$ (*binary*), $b = 8$ (*octal*) , and $b= 16$ (*hexadecimal*) are important for computing and communications
- The ancient Mayans used base 20 and the ancient Babylonians used base 60.

Base b Representations

- We can use positive integer b greater than 1 as a base

Theorem 1: Let b be a positive integer greater than 1. Then if n is a positive integer, it can be expressed uniquely in the form:

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

where k is a nonnegative integer, $a_0, a_1, \ldots.\ a_k$ are nonnegative integers less than b, and $a_k \neq 0$. The a_j, $j = 0, \ldots, k$ are called the base-b digits of the representation.

- The representation of n given in **Theorem 1** is called the ***base b expansion of n*** and is denoted by $(a_k a_{k-1} \ldots. a_1 a_0)_b$.
- We usually omit the subscript 10 for base 10 expansions.

M. Hauskrecht

Binary Expansions

Most computers represent integers and do arithmetic with binary (base 2) expansions of integers. In these expansions, the only digits used are 0 and 1.

Example: What is the decimal expansion of the integer that has $(1\ 0101\ 1111)_2$ as its binary expansion?

Solution:

$(1\ 0101\ 1111)_2 = 1{\cdot}2^8 + 0{\cdot}2^7 + 1{\cdot}2^6 + 0{\cdot}2^5 + 1{\cdot}2^4 + 1{\cdot}2^3 + 1{\cdot}2^2 + 1{\cdot}2^1 + 1{\cdot}2^0 = 351.$

Example: What is the decimal expansion of the integer that has $(11011)_2$ as its binary expansion?

Solution: $(11011)_2 = 1{\cdot}2^4 + 1{\cdot}2^3 + 0{\cdot}2^2 + 1{\cdot}2^1 + 1{\cdot}2^0 = 27$

M. Hauskrecht

Octal Expansions

The octal expansion (base 8) uses the digits $\{0,1,2,3,4,5,6,7\}$.

Example: What is the decimal expansion of the number with octal expansion $(7016)_8$?

Solution: $7 \cdot 8^3 + 0 \cdot 8^2 + 1 \cdot 8^1 + 6 \cdot 8^0 = 3598$

Example: What is the decimal expansion of the number with octal expansion $(111)_8$?

Solution: $1 \cdot 8^2 + 1 \cdot 8^1 + 1 \cdot 8^0 = 64 + 8 + 1 = 73$

M. Hauskrecht

Hexadecimal Expansions

- The hexadecimal expansion uses 16 digits: $\{0,1,2,3,4,5,6,7,8,9,A,B,C,D,E,F\}$.
  - The letters A through F represent the decimal numbers 10 through 15.

Example: What is the decimal expansion of the number with hexadecimal expansion $(2AE0B)_{16}$?

Solution:

$2 \cdot 16^4 + 10 \cdot 16^3 + 14 \cdot 16^2 + 0 \cdot 16^1 + 11 \cdot 16^0 = 175627$

Example: What is the decimal expansion of the number with hexadecimal expansion $(E5)_{16}$?

Solution: $14 \cdot 16^1 + 5 \cdot 16^0 = 224 + 5 = 229$

M. Hauskrecht

Base Conversion

To construct the base b expansion of an integer n:

- Divide n by b to obtain a quotient and remainder.

  $n = bq_0 + a_0 \quad 0 \le a_0 \le b$
- The remainder, a_0, is the rightmost digit in the base b expansion of n. Next, divide q_0 by b.

  $q_0 = bq_1 + a_1 \quad 0 \le a_1 \le b$
- The remainder, a_1, is the second digit from the right in the base b expansion of n.
- Continue by successively dividing the quotients by b, obtaining the additional base b digits as the remainder. The process terminates when the quotient is 0.

M. Hauskrecht

Base Conversion

Example: Find the octal expansion of $(12345)_{10}$

Solution: Successively dividing by 8 gives:

- $12345 = 8 \cdot 1543 + 1$
- $1543 = 8 \cdot 192 + 7$
- $192 = 8 \cdot 24 + 0$
- $24 = 8 \cdot 3 + 0$
- $3 = 8 \cdot 0 + 3$

The remainders are the digits from right to left yielding $(30071)_8$.

M. Hauskrecht

CS 441 Discrete Mathematics for CS
Lecture 14

Mathematical induction & Recursion

Milos Hauskrecht
milos@cs.pitt.edu
5329 Sennott Square

Proofs

Basic proof methods:

- Direct, Indirect, Contradiction, By Cases, Equivalences

Proof of quantified statements:

- **There exists x with some property P(x).**
  - It is sufficient to find one element for which the property holds.
- **For all x some property P(x) holds.**
  - Proofs of 'For all x some property P(x) holds' must cover all x and can be harder.
- **Mathematical induction** is a technique that can be applied to prove the universal statements for sets of positive integers or their associated sequences.

Mathematical induction

- Used to prove statements of the form $\forall x\ P(x)$ where $x \in Z^+$

Mathematical induction proofs consists of two steps:

1) **Basis:** The proposition P(1) is true.
2) **Inductive Step:** The implication

   $P(n) \rightarrow P(n+1)$, is true for all positive n.

- Therefore we conclude $\forall x\ P(x)$.

- **Based on the well-ordering property:** Every nonempty set of nonnegative integers has a **least element**.

Mathematical induction

Example: Prove the sum of first n odd integers is n^2 .

i.e. $1 + 3 + 5 + 7 + ... + (2n - 1) = n^2$ for all positive integers.

Proof:

- What is P(n)? P(n): $1 + 3 + 5 + 7 + ... + (2n - 1) = n^2$

Basis Step Show P(1) is true

- Trivial: $1 = 1^2$

Inductive Step Show if P(n) is true then P(n+1) is true for all n.

- Suppose P(n) is true, that is $1 + 3 + 5 + 7 + ... + (2n - 1) = n^2$
- Show P(n+1): $1 + 3 + 5 + 7 + ... + (2n - 1) + (2n + 1) = (n+1)^2$ follows:
- $\underbrace{1 + 3 + 5 + 7 + ... + (2n - 1)}_{n^2} + (2n + 1) =$

  $n^2 + (2n+1) = (n+1)^2$