Number Theory and Cryptography

Chapter 4

Applications of Congruences

Section 4.5

Section Summary

- Hashing Functions
- Pseudorandom Numbers
- Check Digits

Hashing Functions

Definition: A *hashing function h* assigns memory location $h(k)$ to the record that has k as its key.

- A common [illegible] ing function is $h(k) = k$ **mod** m, where m is the number of memory locations.
- Because [illegible] function is onto, all memory locations are possible.

Example: L [illegible] 111. This hashing function assigns the records of customers with social secu [illegible] to memory locations in the following manner:

h(0642 [illegible] d 111 = 14

h(037149212 [illegible] = 65

h(107405723) = 10 [illegible] but since location 14 is already occupied, the record is assigned to [illegible] n, which is 15.

COVER IT BY
DATA STRUCTURE

- The hashing function is not one-to [illegible] more possible keys than memory locations. When more than one recor [illegible] e location, we say a *collision* occurs. Here a collision has been resolved [illegible] to the first free location.
- For collision resolution, we can use a *linear pro* [illegible]

  $h(k,i) = (h(k) + i)$ **mod** m, where i runs from [illegible]
- There are many other methods of handling with collisions. You [illegible] later CS course.

Pseudorandom Numbers

- **Pseudorandom numbers** are not truly random since they are generated by systematic methods.
- The *linear congruential method* is one commonly used procedure for generating pseudorandom numbers.

- Four integers are needed: the **modulus** m, the **multiplier** a, the ***increment*** c, and **seed** x_0, with $2 \leq a < m$, $0 \leq c < m$, $0 \leq x_0 < m$.
- We generate a sequence of pseudorandom numbers $\{x_n\}$, with $0 \leq x_n < m$ for all n, by successively using the recursively defined function

$$x_{n+1} = (ax_n + c) \textbf{ mod } m.$$

Pseudorandom Numbers

- **Example**: Find the sequence of pseudorandom numbers generated by the linear congruential method with modulus $m = 9$, multiplier $a = 7$, increment $c = 4$, and seed $x_0 = 3$.
- **Solution**: Compute the terms of the sequence by successively using the congruence $x_{n+1} = (7x_n + 4) \mathbf{mod}\ 9$, with $x_0 = 3$.

$$x_1 = 7x_0 + 4 \mathbf{\ mod\ } 9 = 7\cdot 3 + 4 \mathbf{\ mod\ } 9 = 25 \mathbf{\ mod\ } 9 = 7,$$
$$x_2 = 7x_1 + 4 \mathbf{\ mod\ } 9 = 7\cdot 7 + 4 \mathbf{\ mod\ } 9 = 53 \mathbf{\ mod\ } 9 = 8,$$
$$x_3 = 7x_2 + 4 \mathbf{\ mod\ } 9 = 7\cdot 8 + 4 \mathbf{\ mod\ } 9 = 60 \mathbf{\ mod\ } 9 = 6,$$
$$x_4 = 7x_3 + 4 \mathbf{\ mod\ } 9 = 7\cdot 6 + 4 \mathbf{\ mod\ } 9 = 46 \mathbf{\ mod\ } 9 = 1,$$
$$x_5 = 7x_4 + 4 \mathbf{\ mod\ } 9 = 7\cdot 1 + 4 \mathbf{\ mod\ } 9 = 11 \mathbf{\ mod\ } 9 = 2,$$
$$x_6 = 7x_5 + 4 \mathbf{\ mod\ } 9 = 7\cdot 2 + 4 \mathbf{\ mod\ } 9 = 18 \mathbf{\ mod\ } 9 = 0,$$
$$x_7 = 7x_6 + 4 \mathbf{\ mod\ } 9 = 7\cdot 0 + 4 \mathbf{\ mod\ } 9 = 4 \mathbf{\ mod\ } 9 = 4,$$
$$x_8 = 7x_7 + 4 \mathbf{\ mod\ } 9 = 7\cdot 4 + 4 \mathbf{\ mod\ } 9 = 32 \mathbf{\ mod\ } 9 = 5,$$
$$x_9 = 7x_8 + 4 \mathbf{\ mod\ } 9 = 7\cdot 5 + 4 \mathbf{\ mod\ } 9 = 39 \mathbf{\ mod\ } 9 = 3.$$

The sequence generated is 3,7,8,6,1,2,**0,4,5**,3,7,8,6,1,2,**0,4,5,3**,…

It repeats after generating 9 terms.

Check Digits: UPCs

- A common method of detecting errors in strings of digits is to add an extra digit at the end, which is evaluated using a function. If the final digit is not correct, then the string is assumed not to be correct.

Example: Retail products are identified by their **Universal Product Codes** (*UPCs*). Usually these have 12 decimal digits, the last one being the check digit. The check digit is determined by the congruence

$$3x_1 + x_2 + 3x_3 + x_4 + 3x_5 + x_6 + 3x_7 + x_8 + 3x_9 + x_{10} + 3x_{11} + x_{12} \equiv 0 \pmod{10}.$$

a. Suppose that the first 11 digits of the UPC are 79357343104. What is the check digit?

b. Is 041331021641 a valid UPC?

Check Digits: UPCs

$$3x_1 + x_2 + 3x_3 + x_4 + 3x_5 + x_6 + 3x_7 + x_8 + 3x_9 + x_{10} + 3x_{11} + x_{12} \equiv 0 \pmod{10}.$$

a. Suppose that the first 11 digits of the UPC are 79357343104. What is the check digit?

b. Is 041331021641 a valid UPC?

Solution (a):

$3 \cdot 7 + 9 + 3 \cdot 3 + 5 + 3 \cdot 7 + 3 + 3 \cdot 4 + 3 + 3 \cdot 1 + 0 + 3 \cdot 4 + x_{12} \equiv 0 \pmod{10}$

$21 + 9 + 9 + 5 + 21 + 3 + 12 + 3 + 3 + 0 + 12 + x_{12} \equiv 0 \pmod{10}$

$98 + x_{12} \equiv 0 \pmod{10}$

$x_{12} \equiv 2 \pmod{10}$ **So, the check digit is 2.**

Check Digits: UPCs

$3x_1 + x_2 + 3x_3 + x_4 + 3x_5 + x_6 + 3x_7 + x_8 + 3x_9 + x_{10} + 3x_{11} + x_{12} \equiv 0 \pmod{10}$.

a. Suppose that the first 11 digits of the UPC are 79357343104. What is the check digit?

b. Is 041331021641 a valid UPC?

Solution (b):

$3\cdot0 + 4 + 3\cdot1 + 3 + 3\cdot3 + 1 + 3\cdot0 + 2 + 3\cdot1 + 6 + 3\cdot4 + 1$

$0 + 4 + 3 + 3 + 9 + 1 + 0 + 2 + 3 + 6 + 12 + 1 = 44$

$44 \bmod 10 = 4$

$44 \equiv 4 \pmod{10} \not\equiv 0 \pmod{10}$

Hence, 041331021641 is not a valid UPC.

Check Digits : ISBNs

Books are identified by an *International Standard Book Number* (ISBN-10), a 10 digit code. The first 9 digits identify the language, the publisher, and the book. The tenth digit is a check digit, which is determined by the following congruence

$$x_{10} \equiv \sum_{i=1}^{9} i x_i \pmod{11}.$$

The validity of an ISBN-10 number can be evaluated with the equivalent $\sum_{i=1}^{10} i x_i \equiv 0 \pmod{11}.$

a. Suppose that the first 9 digits of the ISBN-10 are 007288008. What is the check digit?

b. Is 084930149X a valid ISBN10?

Check Digits : ISBNs

The validity of an ISBN-10 number can be evaluated with the equivalent $\sum_{i=1}^{10} i x_i \equiv 0 \pmod{11}$.

a. Suppose that the first 9 digits of the ISBN-10 are 007288008. What is the check digit?

b. Is 084930149X a valid ISBN10?

X is used for the digit 10.

Solution:

a. $X_{10} \equiv 1\cdot 0 + 2\cdot 0 + 3\cdot 7 + 4\cdot 2 + 5\cdot 8 + 6\cdot 8 + 7\cdot 0 + 8\cdot 0 + 9\cdot 8 \pmod{11}$.

$X_{10} \equiv 0 + 0 + 21 + 8 + 40 + 48 + 0 + 0 + 72 \pmod{11}$.

$X_{10} \equiv 189 \equiv 2 \pmod{11}$. Hence, $X_{10} = 2$.

b. $1\cdot 0 + 2\cdot 8 + 3\cdot 4 + 4\cdot 9 + 5\cdot 3 + 6\cdot 0 + 7\cdot 1 + 8\cdot 4 + 9\cdot 9 + 10\cdot 10 =$

$0 + 16 + 12 + 36 + 15 + 0 + 7 + 32 + 81 + 100 = 299 \equiv 2 \not\equiv 0 \pmod{11}$

Hence, 084930149X is not a valid ISBN-10.

- A *single error* is an error in one digit of an identification number and a *transposition error* is the accidental interchanging of two digits. Both of these kinds of errors can be detected by the check digit for ISBN-10. (*see text for more details*)

Query???

$$\sqrt{1+\sqrt{2+\sqrt{3+\sqrt{4....}}}}$$

$$\exists_{x \in \Re} \exists_{y \in \Re} (x = y) = ?$$

$$\sum_{x=1}^{\infty} x = ?$$

$$\sum_{x=1}^{\infty} \frac{1}{x} = ?$$

$$\forall_{x} (\Re \mid x) = ?$$

$$\exists_{x \in \Re} \exists_{y \in \Re} (x = y) = ?$$

$$\sqrt{1+\sqrt{2+\sqrt{3+\sqrt{4....}}}} = ?$$

$$1 - 1 + 1 - 1 + 1 .... = ?$$

$$\sum_{x=1}^{\infty} \frac{1}{x} = ?$$