CSI 30 LECTURE NOTES (Ojakian)

Topic 11: Divisibility, Modular Arithmetic, and Crypto

OUTLINE
(References: 4.1, 4.6)

1. Divisibility
2. Modular Arithmetic
3. Cryptography (part 1)

---

1. Divisibility

(a) Divisible: Meaning of $x|b$. "x divides b"
   i. x is a "factor" (or "divisor") of b.

(b) Theorem 1 (page 252). Do proof.

2. Modular Congruence

(a) Example: time on a 24 hour clock: after 23h, what time is it?

(b) Example: memory in C++. For example what is: $65535 + 1$?? (for an unsigned short int we only have 2 bytes)

(c) DEF ("congruence" relation): $a \equiv b(mod\ m)$
Note: distinct from "mod" function (book notation we avoid). And being precise, this is a relation $Z \times Z$.

(d) Equivalent ways to think about congruence.
   i. Theorem 3 (p. 254). Same remainders
   ii. Theorem 4 (p. 255). Can step between (draw number line)
   iii. For congruence mod m, consider the representatives $Z_m = \{0, 1, \ldots, m-1\}$.

3. Modular Arithmetic

Basic moral: Work in Z_m and most all usual rules with addition, subtraction, and multiplication work (avoid standard division ...)

(a) Addition and multiplication rule (Theorem 5 - p. 255)

(b) Substitution rule (Corollary 2 - page 256)

(c) Other typical properties (page 257).
   i. Associativity and Commutativity (i.e. respect order of operations between addition and multiplication, but otherwise can change the order)
   ii. Distributivity
   iii. Additive Inverses. Section 4.1: Exercise 48 (last part)
   iv. Multiplicative Inverses? Wait!

(d) Watch out! - Section 4.1: Exercise 43.

4. Cryptography - Basic setup

   (a) Alice wants to send a secret message to Bob

   (b) But Eve is eavesdropping.

   (c) Competing goals:

      i. Making Codes.
      Alice and Bob want to devise a scheme for sending secret message that Eve cannot gain access to.

      ii. Breaking Codes.
      Eve wants to figure out how to crack the secret and read the hidden message.

   (d) Terminology

      i. Plaintext: The message to be sent (from Alice to Bob), in original form.

      ii. Encryption: Putting plaintext into coded form (Alice does this).

      iii. Decryption: Determining plaintext from coded message (Bob does this); i.e. the inverse of the encryption function.

   (e) To use mathematics:

      i. Use some method for converting natural language to numbers (this is simple translation! not encryption!)

      ii. Example: A = 0, B = 1, etc

5. Cryptography - Shift Cipher

   Simple example. More serious one at later topic.

   (a) Pick a shift value k: $0 < k < 26$.

   (b) Encryption: Letter x is mapped to $x + k \bmod 26$

   (c) Decryption: Letter y is mapped to $y - k \bmod 26$

   (d) Example 5 (Section 4.6): Breaking a code.

   (e) Do group sending, with Alice, Bob, and Eve

6. Affine ciphers: better but they still suck! ...

   (a) Example 3 in section 4.6

7. Exercises

   (a) Section 4.1: 2, 5, 6, 7, 8, 15 - 18

   (b) Section 4.1: 26 - 29 (where "mod" is the same as "%")

   (c) Section 4.1: 30 - 35, 52

   (d) Section 4.6: 1, 2, 3 (also give the result of the encryption BEFORE "translating the numbers back into letters")

   (e) Section 4.6: 4 - 13 (shift and affine ciphers)