CSI 30 LECTURE NOTES (Ojakian)

Topic 11: Divisibility and Modular Arithmetic

OUTLINE

(References: 4.1 and tiny parts of 4.4, 4.5)

1. Divisibility
2. Modular Arithmetic

---

1. Divisibility

(a) Divisible: Meaning of $b|t$. "b divides t" (usual and $\frac{t}{b}$ is integer). Require: $b \neq 0$.
   i. b is a "factor" (or "divisor") of t.

(b) Prove or disprove the following.
   i. 103 divides itself (can use "Universal Instantiation" with next fact).
   ii. Every integer divides itself (the exception?).
   iii. Every integer divides 0 (the exception?).
   iv. If $a|b$ then $a \leq b$

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

(d) Divisibility Proof Exercises (Section 4.1): 6, 7, 8

2. Modular Congruence

(a) Examples on a 24 hour clock. Section 4.1: 16.

(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 using size m steps (draw number line)
   iii. For congruence mod m, consider the representatives $Z_m = \{0, 1, \ldots, m-1\}$.

(e) Examples.
   i. Find the smallest positive integer that is congruent to 37 (mod 10)
   ii. Find the smallest positive integer that is congruent to -37 (mod 10)
   iii. Find the integer x in Z_m such that $x \equiv 16$ (mod 5)

(f) Congruence Exercises. Section 4.1: 34, 35, 30, 31, 32, 33

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.

(e) Exercises. Section 4.1: 17, 18.

(f) Proofs. Section 4.1: 40, 41, 46

(g) Exercises on Z_m. Section 4.1: 48 - 52

4. Modular Inverses (Section 4.4)

(a) Recall: In Z_m, the additive inverse always exists.

(b) Example: In Z_m, find an example of the multiplicative inverse existing and not existing.

(c) Theorem: If a and m are relatively prime, then there is a number q such that

$$aq = 1(mod\ m)$$

(d) Exercises.
Section 4.4: 1 - 4

5. Pseudo Random Numbers (Section 4.5)

Can be generated via linear congruence. Need the following.

(a) Modulus: m. Multiplier: a. Increment: c. Seed: x_0.

(b) Get a sequence of integers $x_0, x_1, \ldots$ (between 0 and $m-1$).

(c) Write a python program to list some number of pseudo-random numbers.

(d) Exercises. Section 4.5: 5, 6, 7