CSI 30 LECTURE NOTES (Ojakian)

Topic 12: Tools For Cryptography

OUTLINE
(References: 4.2, 4.4)

1. Modular Exponentiation (4.2)
2. Modular Inverses (4.4)
3. Fermat's Little Theorem (4.4)
4. Chinese Remainder Theorem (4.4)

---

1. Modular Exponentiation

(a) Modular Multiplication Fact: Second part of Corollary 2, Section 4.1 (page 256).

(b) Example: Calculate $3^6 (mod\ 5)$

i. "From scratch".

ii. "One step at a time" using Modular Multiplication Fact

(c) Using "Fast Modular Exponentiation"

i. Write the exponent in base 2.

ii. Use that to write $b^e = ...$ with corresponding powers of 2.

iii. Calculate b to these powers of 2 by successive squaring mod m, starting with just b.

iv. Multiply everything mod m

(d) Exercises.

i. Find $3^{11} (mod\ 4)$ all 3 ways: from scratch, one-step at a time, and fast exponentiation (only use a calculator for from scratch)

ii. Find $4^{21} (mod\ 10)$ using fast exponentiation

iii. Section 4.2: 25 - 28

2. Solving Modular Equations

(a) Consider solving standard equations. Example: $2x = 7$.

(b) Do same, but now for modular equivalence.

i. Form: $ax \equiv b (mod\ m)$

(c) Exercises.
Section 4.4: 9, 10 (just solve from scratch)

3. Modular Inverses

   (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

4. Fermat's Little Theorem

   If p is a prime which does *not* divide a, then $a^{p-1} \equiv 1(mod\ p)$

   (a) Exercises.
   Section 4.4: 33 - 36

5. Chinese Remainder Theorem

   (a) Recall usual system of equations.
      i. Example: Solve $x^2 = 9$ and $2x = -6$

   (b) For modular system.
      i. Solve the system $x \equiv 1(mod\ 2)$ and $x \equiv 2(mod 3)$

   (c) Theorem 2 (section 4.4, page 294). Just for TWO congruences:
   Suppose $m_1, m_2 \geq 2$ are relatively prime integers. The system

   $$x \equiv a_1(mod\ m_1), \quad x \equiv a_2(mod\ m_2)$$

   has a unique solution mod $m_1 \cdot m_2$.

   (d) Exercises.
      i. Pick small numbers and verify.
      ii. Section 4.4: 37