CSE 20 Homework 8
Due: Saturday December 9 2017 at **11pm**

Topics Equivalence relations, congruence mod m, and applications.

Reading Rosen Sections 9.1, 9.5, 4.1, 4.5, 4.6

Key Concepts Binary relations, reflexivity, symmetry, transitivity, equivalence relation, partition, equivalence class, congruence modulo m, modular arithmetic, applying modular arithmetic to hash functions, applying modular arithmetic to ciphers.

1. (**14 points**)

(a) For each of the following relations R on the given domains A, categorize them as not an equivalence relation, an equivalence relation with finitely many distinct equivalence classes, **or** an equivalence relation with infinitely many distinct equivalence classes. Justify each decision with a brief proof.

(i) $A = \{1, 2, 3\}$, $R = \{(1, 1), (2, 2), (3, 3)\}$

(ii) $A = \mathbb{R}$, $R = \{(x, y) \mid x^2 = y^2\}$

(iii) $A = \mathbb{Z}$, $R = \{(x, y) \mid x \equiv y \pmod 4\}$

(iv) $A = \mathcal{P}(\mathbb{Z}^+)$, $R = \{(x, y) \mid x \subseteq y\}$

(b) Comparing the congruence class of 6 modulo 8 and the congruence class of 6 modulo 12, which of the following is true? Prove the statement if true; disprove it if false.

(i) $[6]_8 \subseteq [6]_{12}$

(ii) $[6]_{12} \subseteq [6]_8$

(iii) $[6]_8 \cap [6]_{12} = \emptyset$

2. (**12 points**)

(a) Prove that for all integers n, n^2 does not have remainder 2 upon division by 3.

(b) Compute the last digit of $(23)^{7102}$. Justify your answer using modular arithmetic; do not simply plug in the numbers into a calculator.

3. (**8 points**) *Read the introduction to hashing functions on page 287 of the textbook.* A commonly used **hashing function** for assigning memory addresses to records is $h : \{\text{possible input records}\} \to \{0, \dots, m-1\}$ and

$$h(k) = k \mod m$$

where m is the number of available memory locations. This function is **onto** the codomain of possible memory locations $\{0, \dots, m-1\}$ but may not be one-to-one. Two input values a, b where $a \neq b$ but $h(a) = h(b)$ result in a **collision**.

(a) Which memory locations are assigned by the hashing function $h(k) = k \mod 310$ to the records given by Social Security numbers

(i) 104578690

(ii) 372201919

(b) Find a Social Security number that would cause a collision (under this same hashing function) with one of the numbers above. Use only valid Social Security numbers, as described (by Wikipedia) as

> Prior to June 25, 2011, a valid SSN could not have an area number between 734 and 749, or above 772, the highest area number the Social Security Administration has allocated. Effective June 25, 2011, the SSA assigns SSNs randomly and allows for the assignment of area numbers between 734 and 749 and above 772 through the 800s . . . Some special numbers are never allocated:
>
> – Numbers with all zeros in any digit group (000-##-####, ###-00-####, ###-##-0000).
>
> – Numbers with 666 or 900-999

Justify your answer.

4. (**8 points**) *Read the introduction to cryptographic protocols on page 302 of the textbook.*
Cryptography is the process of hiding a message by encoding it in a reverseable (decodable) way. Many cryptographic schemes rely on modular arithmetic. Often, the two parties who want to communicate in secret need to share a common piece of information, called a key. Since messages are often encoded as numbers, the key is typically an integer. The Diffie-Hellman algorithm lets Alice and Bob agree on a shared secret number, without each one revealing their own secret to the other. Here is the algorithm:

- Alice and Bob agree (in public) to use a prime p and an integer a with $0 \leq a < p$.

  The numbers p and a are not secret.
- Alice chooses a secret integer k_1 and sends $y_a = a^{k_1} \mod p$ to Bob.
- Bob chooses a secret integer k_2 and sends $y_b = a^{k_2} \mod p$ to Alice.
- Alice computes $(y_b)^{k_1} \mod p$.
- Bob computes $(y_a)^{k_2} \mod p$.

Note: in order for this to work properly, we need additional assumptions on a; see textbook for details.

(a) Describe each step (write out the results of all computations) that Alice and Bob follow when they use the Diffie-Hellman key exchange protocol to generate a shared key, using the prime $p = 19$ and $a = 2$. Assume that Alice selects $k_1 = 11$ and Bob selects $k_2 = 5$. *You may use a calculator, MATLAB, Wolfram Alpha, etc. so long as you include the results of intermediate calculations.*

(b) What's Alice and Bob's shared secret number in this case? Explain why they each got the same number.

Bonus - not for credit: read more about different cryptographic schemes in Section 4.5 in the book.