CSE 20, Fall 2020 - Homework 8

Due: Monday 12/7 at 11 am PDT

Instructions

Upload a single file to Gradescope for each group. All group members' names and PIDs should be on each page of the submission. You should select appropriate pages for each question when submitting to Gradescope. Your assignments in this class will be evaluated not only on the correctness of your answers, but on your ability to present your ideas clearly and logically. You should always explain how you arrived at your conclusions, using mathematically sound reasoning. Whether you use formal proof techniques or write a more informal argument for why something is true, your answers should always be well-supported. Your goal should be to convince the reader that your results and methods are sound.

Reading Definitions 1-5 Section 9.1 (pp. 574-578) -Binary Relation, Relation on a Set, Reflexivity, Symmetry, Transitivity; Definitions 1, 3 Section 9.5 (p. 609), Definition of partition, Section 9.6 (p. 612)

Key Concepts Equivalence Relations; Modular arithmetic

Problem 1 (20 points)

For each of the following relations R on the set of natural numbers $\mathbb{N}$, determine if it is symmetric or not. **Prove your answer**.

1. $R = \{(a,b) \mid a - b \leq 1\}$
2. $R = \{(a,b) \mid a \neq b\}$

Problem 2 (20 points)

Is intersection of two equivalence relations itself an equivalence relation? **Prove your answer.**

Problem 3 (20 points)

For each of the following relations R on the set of real numbers $\mathbb{R}$, determine if it is transitive or not. **Prove your answer**.

1. $R = \{(a,b) \mid |a - b| \leq 1\}$
2. $R = \{(a,b) \mid a \leq b\}$

Problem 4 (20 points)

Let f**:** $C \to D$ be a function and let R_f be the binary relation on C defined by:

$$R_f = \{(x,\ y) \mid f(x)\ = f(y)\}$$

a. Prove that R_f is an equivalence relation
b. For each of the two scenarios listed below, answer all of the following questions OR state that there is not enough information to tell:
    - Is D finite?
    - Is f one-to-one?
    - Is f onto?

    Please briefly justify your answer for each question.

    Two scenarios:

    1. C is finite, and R_f partitions C into |C| equivalence classes
    2. C is finite, and R_f partitions C into |D| equivalence classes

Problem 5 (20 points)

Prove by induction on integer $n \geq 0$ that for any integers $a, b, c \geq 1$ we have:
$(a^b \mod c)^n \mod c = a^{bn} \mod c$

Note: This result above guarantees that under the Diffie-Hellman key exchange protocol that we learned in class, the key $A^{k_2} \, mod\, p$ (with $A = a^{k_1} \, mod\, p$) computed by Alice and the key $B^{k_1} \, mod\, p$ (with $B = a^{k_2} \, mod \; p$) computed by Bob are the same.

Problem 6 - Bonus (10 points)

Let S be a set of size |S| = 5.

a. How many binary relations on S are there?
b. How many reflexive binary relations on S are there?
c. How many symmetric binary relations on S are there?