Review Guide: Chapter 8

Definitions: How are the following terms defined?

- congruence modulo 2 relation *(p. 443)*
- inverse of a relation from a set A to a set B *(p. 444)*
- relation on a set *(p. 446)*
- directed graph of a relation on a set *(p. 446)*
- n-ary relation (and binary, ternary, quaternary relations) *(p. 447)*
- reflexive, symmetric, and transitive properties of a relation on a set *(p. 450)*
- congruence modulo 3 relation *(p. 455)*
- transitive closure of a relation on a set *(p. 457)*
- equivalence relation on a set *(p. 462)*
- equivalence class *(p. 465)*
- congruence modulo n relation *(p. 471)*
- representative of an equivalence class *(p. 472)*
- m is congruent to n modulo d *(p. 473)*
- plaintext and cyphertext *(p. 478)*
- residue of a modulo n *(p. 481)*
- d is a linear combination of a and b *(p. 486)*
- a and b are relatively prime; $a_1, a_2, \ldots, a_n$ are pairwise relatively prime *(p. 488)*
- an inverse of a modulo n *(p. 489)*
- antisymmetric relation *(p. 499)*
- partial order relation *(p. 500)*
- lexicographic order *(p. 502)*
- Hasse diagram *(p. 503)*
- a and b are comparable *(p. 505)*
- poset *(p. 506)*
- total order relation *(p. 506)*
- chain, length of a chain *(p. 506)*
- maximal element, greatest element, minimal element, least element *(p. 507)*
- topological sorting *(p. 507)*
- compatible partial order relations *(p. 508)*
- PERT and CPM *(p. 510)*
- critical path *(p. 512)*

Properties of Relations on Sets and Equivalence Relations

- How do you show that a relation on a finite set is reflexive? symmetric? transitive? *(pp. 450-452)*
- How do you show that a relation on an infinite set is reflexive? symmetric? transitive? *(pp. 453-456)*
- How do you show that a relation on a set is not reflexive? not symmetric? not transitive? *(pp. 451-454)*
- How do you find the transitive closure of a relation? *(p. 457)*
- What is the relation induced by a partition of a set? *(p. 460)*
- Given an equivalence relation on a set A, what is the relationship between the distinct equivalence classes of the relation and the set A? *(p. 469)*
- In what way are rational numbers equivalence classes? *(pp. 473-474)*

Cryptography

- How does the Caesar cipher work? *(p. 478)*
- If a, b, and n are integers with $n > 1$, what are some different ways of expressing the fact that $n \mid (a - b)$? *(p. 480)*
- If n is an integer with $n > 1$, is congruence modulo n an equivalence relation on the set of all integers? *(p. 481)*
- How do you add, subtract, and multiply integers modulo an integer $n > 1$? *(p. 482)*
- What is an efficient way to compute a^k where a is an integer with $a > 1$ and k is a large integer? *(pp. 484-485)*
- How do you express the greatest common divisor of two integers as a linear combination of the integers? *(p. 487)*
- When can you find an inverse modulo n for a positive integer a, and how do you find it? *(pp. 488-489)*
- How do you encrypt and decrypt messages using RSA cryptography? *(pp. 491-492)*
- What is Euclid's lemma? How is it proved? *(p. 492)*
- What is Fermat's little theorem? How is it proved? *(p. 494)*
- Why does the RSA cipher work? *(pp. 494-496)*

Partial Order Relations

- How do you show that a relation on a set is or is not antisymmetric? *(pp. 499-500)*
- If A is a set with a partial order relation R, S is a set of strings over A, and a and b are in S, how do you show that $a \preceq b$, where $\preceq$ denotes the lexicographic ordering of S? *(p. 502)*
- How do you construct the Hasse diagram for a partial order relation? *(p. 503)*
- How do you find a chain in a partially ordered set? *(p. 506)*
- Given a set with a partial order, how do you construct a topological sorting for the elements of the set? *(p. 508)*
- Given a job scheduling problem consisting of a number of tasks, some of which must be completed before others can be begun, how can you use a partial order relation to determine the minimum time needed to complete the job? *(pp. 511-512)*