Problem Set 3

Due: Start of Class, September 26.

Reading: Sections 1.4–1.5, 2.4–2.5, 3.3, and 6.1–6.2 of *Discrete Mathematics and its Applications* by Kenneth H. Rosen.

Problem 3-1. We are given two buckets A and B of capacities a and b, a water hose, a receptacle, and a drain. The receptacle can be used to store an unlimited amount of water. Of course, the receptacle has no measurement markings. Excess water can be dumped into the drain. Consider the following "Die Hard" operations:

- fill bucket A or bucket B from either the hose or the receptacle
- empty bucket A or bucket B to the drain or the receptacle
- pour from A to B until either A is empty or B is full
- pour from B to A until either B is empty or A is full

Let $c = gcd(a, b)$. Prove that we can put g gallons into the receptacle using the above operations if, and only if, $c \mid g$. Give an explicit scheme for putting exactly 14 ounces of water into the receptacle (the final holder) using a 133 ounce and a 49 ounce bucket.

Problem 3-2. Read the description of the RSA cryptosystem from the textbook, pp 146-148.

(a) Given primes $p = 173$ and $q = 149$ generate encyption and decription keys, e and d respectively, such that $e \cdot d = 1 \bmod (p-1)(q-1)$. For "security," make $e, d \geq 20$.

(b) Convert the word "MIT" to a number by first mapping each letter to its position in the alphabet, e.g. A = 0, B = 1, C = 2, …, Z = 25, and then gathering the numbers (M, I, T) into a single number $26^2 * M + 26 * I + T$. Find the RSA-encrypted version of "MIT" and show that it decrypts properly.

(c) What happens when you apply the encrypt/decrypt operation to "YOU"? Why?

Problem 3-3. The least common multiple of two natural numbers, m and n is defined to be the smallest natural number k such that $m|k$ and $n|k$. It is denoted by $lcm(m, n)$. Prove that every pair of natural numbers has a least common multiple. Using unique factorization, show that $a \cdot b = gcd(a, b) \cdot lcm(a, b)$.

Problem 3-4. Sets.

(a) Show that $A \cap (A \cup B) = A$.

(b) Prove: if $P(A) = P(B)$ (identical power sets), then $A = B$.

(c) Find the error in the "proof" of the following "theorem."

> **Theorem 0.1** *Let R be a relation on a set A that is symmetric and transitive. Then R is reflexive.*
>
> *Proof.* Let $a \in A$. Take an element $b \in A$ such that $(a, b) \in R$. Since R is symmetric, we also have $(b, a) \in R$. Now using the transitive property, we can conclude that $(a, a) \in R$ since $(a, b) \in R$ and $(b, a) \in R$. ∎

Problem 3-5. Cartesian Products. Let A and B be any sets.

(a) Prove that $(A \times B) \cap (B \times A) = (A \cap B) \times (A \cap B)$

(b) Prove that $(A \times B) \cup (B \times A) \subseteq (A \cup B) \times (A \cup B)$

(c) Give an example to show that equality in the previous statement is not always achieved.

Problem 3-6. Example 8 of section 3.2 shows that every set of n elements contains 2^n subsets. Prove by induction that any set containing $n > 0$ elements has exactly 2^{n-1} subsets of even size (for example, $\{1, 2\}$ has two subsets of even size: $\emptyset$ and $\{1, 2\}$).