Math 173A - Homework 1

1. Do the following exercises from the textbook. 1.8, 1.10 (applied to 1.9b), 1.11, 1.18, 1.20, 1.27, 1.28.

2. Prove that a number is divisible by 3 if and only if the sum of its digits (written in base 10) is divisible by 3. *Hint: write* $10 = 9 + 1$ *and apply the binomial theorem.*

3. Prove that modular inverses are unique. That is, fix a positive integer m and suppose $\gcd(a, m) = 1$. Show that if $ab_1 \equiv ab_2 \equiv 1 \pmod{m}$, then $b_1 \equiv b_2 \pmod{m}$.

4. In this problem we'll count the number of simple substitution ciphers on an alphabet, Σ, of size n that leave no letter fixed.

   (a) Let S be the set of all permutations $\Sigma \to \Sigma$ that fix at least one letter. Write an expression for the number of permutations that fix no letter in terms of $|S|$.

   (b) Let S_i be the set of permutations that fix the i-th letter of the alphabet. Write S in terms of the S_i's.

   (c) What is $|S_i|$? What about $|S_i \cap S_j|$ for $i \neq j$? What about a k-fold intersection like $|S_{i_1} \cap S_{i_2} \cap \cdots \cap S_{i_k}|$.

   (d) Let $A_1, A_2, \ldots, A_k$ be sets. Draw Venn diagrams illustrating how to compute $|A_1 \cup A_2|$ and $|A_1 \cup A_2 \cup A_3|$ in terms of $|A_1|$, $|A_2|$, $|A_3|$. Use this idea to compute (and prove your answer) $|A_1 \cup A_2 \cup \cdots \cup A_k|$.

   (e) Using the previous parts of this exercise, compute the number of permutations that fix no letter.

   (f) Choose a permutation uniformly at random (that is, each permutation is equally likely to be chosen). What is the probability that it fixes no letter? What happens to this probability as the size of the alphabet approaches infinity? Is this intuitive?