Math 2001: Homework 9

Due: November 5, 2008

Give complete justifications for all your answers.

Problem 1

1. The book proves that the period of the last digit in the Fibonacci sequence is 60 (Theorem 2.3.4). Use this theorem to find the period of the last two digits.
2. Give two ways to partition the set of subsets of $\{1, 2, 3, 4, 5\}$ into 3 parts.

Problem 2

1. Suppose my public key is $(4087, 7)$. Suppose you want encrypt the number 100. What number would you send me (you may wish to use a calculator)?
2. Suppose you have two primes 29 and 71 and you have chosen your public key to be $(2059, 53)$. Suppose I send you the encrypted number 1216. What number did I send you? (You may wish to use a calculator). Hint: I picked 53, so that the first guess for an inverse in $\mathbb{Z}_{1960}$ should be correct.

Problem 3

Let R_n be the set of ways to place n non-attacking rooks on an $n \times n$ chess-board.

1. Prove that $|R_n| = n!$ using induction.
2. Let $f : R_n \to \mathbb{Z}$ be given by

   $$f(r) = \text{number of rooks on the diagonal squares of } r, \qquad \text{for } r \in R_n.$$

   For example, if $n = 4$,

   $$f\left(\begin{array}{|c|c|c|c|}\hline \text{♖} & & & \\ \hline & * & & \text{♖} \\ \hline & & \text{♖} & \\ \hline & \text{♖} & & * \\ \hline\end{array}\right) = 2,$$

   where I've marked the diagonal squares with $*$.

   (a) What is $f(R_n)$?

   (b) Is f injective?

   (c) Is f surjective?

   (d) Is there a partition of R_n described by f?
3. Find an injective function $g : R_n \to \mathbb{Z}$.