SOAR Math Course Homework Five Spring, 2003

These homework problems are meant to expand your understanding of what goes on during class. Any you turn in will be graded and returned to you. Answers may or may not be posted on the web, depending on demand.

1. These problems involve mathematical induction. That is, see if you can prove these using induction, as done in class.

   (a) Show that $\sum_{k=1}^{n}(2k-1) = n^2$.

   (b) Show that $\sum_{k=1}^{n} k^2 = \frac{n(n+1)(2n+1)}{6}$.

   (c) Show that $\sum_{k=1}^{n} k^3 = \left(\frac{n(n+1)}{2}\right)^2$.

   (d) Let $F(n)$ be the nth Fibonacci number. That is, $F(1) = 1$, $F(2) = 1$, and $F(n) = F(n-1) + F(n-2)$ for $n \geq 3$. Show that $\sum_{k=1}^{n} F(k)^2 = F(n)F(n+1)$.

   (e) Show that $2^{2^n} + 3^{2^n} + 5^{2^n}$ is divisible by 19 for every $n \geq 1$. (Hint: prove that if this is true for n then it is also true for $n+2$. You will need two base cases here – one for odd n and the other for even n.)

2. I claimed today that the fifth Fermat number, $F_5 = 2^{2^5} + 1$, is not prime. Factor this number. (This was done by Euler in 1732. You may use resources that Euler did not have available, such as electricity. Please don't simply use the web, though; try to factor this yourself.)

3. On Friday at 3:00 PM, I will publish on the web page a public key and an encrypted message. I will encrypt the message using $A = 01$, $B = 02$, up through $Z = 26$ and space as 27 and concatenate a fixed number of characters at a time. I will not use lower-case letters or punctuation.

   (a) Decrypt the message using my public key.

   (b) Factor my product of two primes and send me a message encrypted using my key.

   (c) Make up your own public and private key and email me a message with these keys. I will post the message and the public key on the web page. (I may restrict the size of the primes permitted.) *Your key and message are due by the start of class next week.*

   (d) Next week, decrypt everyone else's messages.

   (e) If possible, "break" other people's code and email me a message using their private key. (Also send me a factorization of their product of two primes.)

   This is something of a race. Prizes may or may not be awarded.

A Puzzle

This problem was given to me by another post-doctoral fellow. He's interested in knowing the general answer (part (d)).

Consider the rearrangements of the numbers from 1 to n. For example, consider $\{1\ 3\ 2\}$ (so here $n = 3$). There is one "decrease" in that: from 1 to 3 is an increase, but 3 to 2 is a decrease. To each re-arrangement, we assign $+1$ if there are an *even* number of decreases, and -1 if there are an odd number. So our example $\{1\ 3\ 2\}$ would be assigned -1.

Now let $S(n)$ be the sum of these values of $+1$ and -1 over all $n!$ possible re-arrangments of $\{1\ 2\ 3\ \ldots\ n\}$. We'll compute $S(3)$: the $3! = 6$ re-arrangements are:

$$\begin{array}{lll} \{1\ 2\ 3\} = +1 & \{1\ 3\ 2\} = -1 & \{2\ 1\ 3\} = -1 \\ \{2\ 3\ 1\} = -1 & \{3\ 1\ 2\} = -1 & \{3\ 2\ 1\} = +1 \end{array}$$

Summing these six numbers, we get $S(3) = +1 - 1 - 1 - 1 - 1 + 1 = -2$.

(a) Compute $S(2)$.

(b) Compute $S(4)$.

(c) Compute $S(n)$ for n even. (Hint: can you group the re-arrangements in a way that makes the sum simple?)

(d) Compute $S(n)$ for n odd. (This is what my friend would like an answer for. He and I currently don't know a general form for $S(n)$. We do know the answer to part (c), though.)