SOAR Math Course Homework Ten 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. We saw in class today that there are $\phi(p-1)$ primitive roots modulo p. Since $\phi(10) = 4$, there should be 4 primitive roots modulo 11. Find them. (Recall that a base b is a primitive root modulo p if $b^{p-1} \equiv 1 \bmod p$ but $b^k \not\equiv 1 \bmod p$ for $1 < k < p-1$.)

2. Let n be an odd number, not necessarily prime. Show that $\left(\frac{-1}{n}\right) = (-1)^{(n-1)/2}$ as follows.

   (a) Write $n = p_1 p_2 \cdots p_k$ as a product of odd (not necessarily distinct) primes. Show that
   $$\left(\frac{-1}{n}\right) = (-1)^{\sum_j \frac{p_j-1}{2}}.$$

   (b) Write $n = p_1 p_2 \cdots p_k$ as
   $$n = (1 + (p_1 - 1))(1 + (p_2 - 1)) \cdots (1 + (p_k - 1))$$
   and show that this simplifies to
   $$n = 1 + \sum_{j=1}^{k} (p_j - 1) + 4K$$
   for some integer K. (Use the fact that each p_j is odd, so $p_j - 1$ is even. You may assume that there are at least two primes – so $k \geq 2$ – as the $k = 1$ case is simply $n = p_1$.)

   (c) Conclude from part (b) that $(-1)^{\sum_j \frac{p_j-1}{2}} = (-1)^{(n-1)/2}$, so that $\left(\frac{-1}{n}\right) = (-1)^{(n-1)/2}$.

3. Use the previous problem to show that
$$\left(\frac{-1}{n}\right) = \begin{cases} 1 & \text{if } n \equiv 1 \bmod 4, \text{ or } n = 4k+1 \\ -1 & \text{if } n \equiv 3 \bmod 4, \text{ or } n = 4k+3 \end{cases}$$

4. (a) Use the fact that $\left(\frac{2}{n}\right) = (-1)^{(n^2-1)/8}$ (where $n \geq 3$ is odd) to show that
$$\left(\frac{2}{n}\right) = \begin{cases} 1 & \text{if } n \equiv \pm 1 \bmod 8, \text{ or } n = 8k \pm 1 \\ -1 & \text{if } n \equiv \pm 3 \bmod 8, \text{ or } n = 8k \pm 3 \end{cases}$$

   (b) [Hard without an outline] Use an argument as in problem 1 to show that the formula used in part (a) for $\left(\frac{2}{n}\right)$ is correct.

5. Suppose m and n are odd and relatively prime (that is, $\gcd(m,n) = 1$). Use the fact that
$$\left(\frac{m}{n}\right)\left(\frac{n}{m}\right) = (-1)^{\frac{m-1}{2}\frac{n-1}{2}}$$
to compute $\left(\frac{m}{n}\right)\left(\frac{n}{m}\right)$. There are four possibilities for the odd numbers m and n. That is, $m \equiv 1 \bmod 4$ or $m \equiv 3 \bmod 4$ (and similarly for n) combine for four situations. Describe $\left(\frac{m}{n}\right)\left(\frac{n}{m}\right)$ in all these cases.

6. Let F_k be the Fibonacci numbers and L_k be the Lucas numbers. That is, $F_0 = 0$, $F_1 = 1$, and $F_n = F_{n-1} + F_{n-2}$ for $n \geq 2$. Similarly, $L_0 = 2$, $L_1 = 1$, and $L_n = L_{n-1} + L_{n-2}$ for $n \geq 2$.
   (a) Use induction to show that $L_n = (F_{n+1} + F_{n-1})/2$ for $n \geq 1$.
   (b) Use induction to show that $F_n = (L_{n+1} + L_{n-1})/5$ for $n \geq 1$.

The group of the week this week is called S_n. This is the group of *permutations* (or re-arrangements) of the first n numbers $\{1, 2, 3, \ldots, n-1, n\}$. For this reason it is called the *permutation group*.

We will write an element of S_n as, for example, $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 5 & 4 & 2 \end{pmatrix}$. This is an element of S_5, and it is the re-arrangement that sends 1 to 3, 2 to 1, 3 to 5, and 5 to 2. This particular element does not move 4.

We "multiply" elements of S_n by simply doing the re-arrangements one after the other. In S_4, the product $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$ can be constructed as

$$\begin{array}{cccc} 1 & 2 & 3 & 4 \\ \downarrow & \downarrow & \downarrow & \downarrow \\ 2 & 3 & 4 & 1 \\ \downarrow & \downarrow & \downarrow & \downarrow \\ 1 & 2 & 4 & 3 \end{array}$$

That is, in the product $A * B$, we first do the permutation B, then follow up with the permutation A. We've just shown that
$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 4 & 3 \end{pmatrix}.$$

7. The six elements of S_3 are:
$$1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \quad a = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \quad b = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \quad c = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix},$$
$$d = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \quad \text{and} \quad f = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

(a) Write down the multiplication table for S_3 using the notation $\{1, a, b, c, d, f\}$ for the six elements.

(b) Using part (a), show by example that $x * y$ is not always the same as $y * x$ in S_n. [This shows that S_n is not necessarily commutative (or abelian). (See Homework 9, Problem 10 for the terminology.)]

8. How many elements are there in S_n? (That is, how many possible ways can one re-arrange, or permute, the n numbers from 1 to n?)

The groups S_n is an excellent collection of groups to study, since all finite groups can be thought of as subgroups of some S_n. How? A group G with n elements can be expressed as a subgroup of S_n by numbering each of the elements 1 to n. Then each element of G corresponds (through the group multiplication) to a re-arrangement (or permutation) of 1 through n, or an element of S_n!