SOAR Math Course Homework Five Winter, 2002

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 say that two objects have the *same symmetry type* if their symmetry groups are isomorphic and that, under the isomorphism, rotations correspond to rotations and reflections correspond to reflections. Prove that

   (a) the groups C_2 and D_1 are isomorphic, but...

   (b) C_2 and D_1 are not the same symmetry type.

2. Let n be a positive integer, and let G be the set

$$G = \{k \ : \ k \text{ is an integer with } 0 < k < n \text{ and } \gcd(k, n) = 1\}.$$

   Prove that G is a group with operation $\otimes$ multiplication modulo n as follows:

   (a) Prove that 1 is an element of G. (This is easy. You may also assume associativity holds.)

   (b) Prove that G is closed. That is, show that if k and l are integers with $0 < k, l < n$ and $\gcd(k, n) = \gcd(l, n) = 1$, show that $\gcd(kl, n) = 1$ and so $\gcd(k \otimes l, n) = 1$. (Warning! Recall that $k \otimes l \neq kl$, only that $k \otimes l \equiv kl \bmod n$, so that $k \otimes l = kl$ minus some integer multiple of n.)

   (c) Prove that every element of G has an inverse. Here's a handy sketch for you to fill in: Suppose that $a \otimes b = a \otimes c$ for some elements a, b, and c in G. If we can show that $b = c$, then we've shown that the product of a with elements of G produces a permutation of the elements of G. In particular, $a \otimes d = 1$ for some d in G, so $d = a^{-1}$. That is, a has an inverse.

   So how do we prove that $b = c$? Since $a \otimes b = a \otimes c$, we have $ab \equiv ac \bmod n$, or $a(b - c) = kn$ for some integer k. Since $\gcd(a, n) = 1$, what does that say about $b - c$?

3. Use the result of the previous problem to prove the *Chinese Remainder Theorem*:

   If m and n are positive integers with $\gcd(m, n) = 1$, then there are integers a and b with $am + bn = 1$.

   Hint: You may assume that $m < n$. Then in the previous problem let $k = m$ and $n = n$. What does the Chinese Remainder Theorem say about m?