SOAR Math Course Homework Eleven 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. Recall that the symbol $\left(\frac{m}{n}\right)$ means the Legendre symbol or more generally the Jacobi symbol, as last week. Compute the following Legendre symbols:

$$\text{(a)}\ \left(\frac{5}{7}\right) \qquad \text{(b)}\ \left(\frac{2}{5}\right) \qquad \text{(c)}\ \left(\frac{2}{3}\right) \qquad \text{(d)}\ \left(\frac{3}{11}\right)$$

2. Compute the following Jacobi symbols:

$$\text{(a)}\ \left(\frac{125}{7}\right) \qquad \text{(b)}\ \left(\frac{5}{21}\right) \qquad \text{(c)}\ \left(\frac{2}{15}\right)$$

   You may use the facts that $\left(\frac{ab}{n}\right) = \left(\frac{a}{n}\right)\left(\frac{b}{n}\right)$ and $\left(\frac{a}{mn}\right) = \left(\frac{a}{m}\right)\left(\frac{a}{n}\right)$. You may also wish to recall that $\left(\frac{a}{n}\right) = \left(\frac{b}{n}\right)$ if $a \equiv b \bmod n$.

3. With normal fractions, $\frac{m}{n}\frac{n}{m} = 1$. This is not true for Jacobi symbols.

   (a) Show by example that sometimes $\left(\frac{m}{n}\right)\left(\frac{n}{m}\right) = 1$. (Hint: use problems 1(a)(b) and the fact that $\left(\frac{a}{n}\right) = \left(\frac{b}{n}\right)$ if $a \equiv b \bmod n$.)

   (b) Show by example that sometimes $\left(\frac{m}{n}\right)\left(\frac{n}{m}\right) = -1$. (Hint: use problems 1(c)(d).)

   (c) In fact, the rule is

$$\left(\frac{m}{n}\right)\left(\frac{n}{m}\right) = (-1)^{\frac{m-1}{2}\frac{n-1}{2}}$$

   whenever m and n are odd, positive integers with $\gcd(m, n) = 1$. Show that your examples in parts (a) and (b) satisfy this rule.

   (d) Suppose m and n are odd numbers. When is $\left(\frac{m}{n}\right)\left(\frac{n}{m}\right) = +1$ and when is $\left(\frac{m}{n}\right)\left(\frac{n}{m}\right) = -1$? The answer I'm looking for should involve all the possibilities: when $m \equiv 1 \bmod 4$, when $m \equiv 3 \bmod 4$, and when $n \equiv 1$ or $3 \bmod 4$.

4. A composite number n will only pass the strong probable prime test for less than one-quarter of the bases b from 2 to $n - 1$. Thus if we pick a base at random, a composite number will pass the strong test 25% of the time. If we choose *two* bases at random, then a composite number will pass the strong test for these two bases $(1/4)^2 = 1/16 = 6.25\%$ of the time.

   (a) What is the probability that a number n which passes the strong test for 8 randomly chosen bases is composite?

   (b) How many bases would we need to choose randomly to ensure that a composite number passes the strong test with probability less than $10^{-10} = 10^{-8}\% = 0.000\,000\,01\%$. [Skip this problem if you've never seen logarithms.]

5. Use the Lucas-Lehmer test to show that $2^{11} - 1 = 2047$ is not prime. (Here $n = 11$, so I'm asking you to show that $L_{10} \not\equiv 0 \bmod 2047$.)

6. The number $n = 251 = 1 + 2 \cdot 5^3$ is prime.

   (a) Show that n passes the Lucas-Lehmer test with $x = 11$. That is, show that $11^{(251-1)/2} \equiv -1 \bmod 251$ and $11^{(251-1)/5} \not\equiv 1 \bmod 251$.

   (b) Let x be any prime less than 11. Show that n fails the Lucas-Lehmer test for this x. That is, show that either $x^{(251-1)/2} \not\equiv -1 \bmod 251$ or $x^{(251-1)/5} \equiv 1 \bmod 251$.

The group of the week this week is the symmetry group of the cube. For these problems, it is best to have a cube handy to look at and play with. (For example, a die or a Rubik's cube would be nice. You can also fold one out of a sheet of paper – see the web page for links to some web pages with templates for constructing models.)

7. Number the corners of a cube, 1 through 8. Write down all of the symmetries of the cube in terms of what happens to the corners. (Note: we're interested only in symmetries that one can do with a sample cube. That is, we are not counting reflections that involve turning the cube inside out. We only want *orientation-preserving* symmetries, and we exclude *orientation-reversing* symmetries.)

8. Let us write all the symmetries in terms of two of them. Lay the cube flat on a table, so that the top and bottom are parallel to the ground. Our first symmetry (we'll call it r) is a quarter-turn rotation of the cube parallel to the ground. (Make the rotation counter-clockwise when looking down on the cube.) The second symmetry (call it f) is to flip the cube upside-down, so that the top becomes the bottom and vice versa. Facing the front of the cube, let's say that f is a half-turn.

   (a) Let's write rf to mean first f, then r. Similarly, fr^2 means first r twice, then f. For what value of k is $rf = fr^k$?

   (b) Identify each of your symmetries from the previous problems in terms of r and f.

   (c) Find the smallest positive values of k and n for which $r^k = 1$ and $f^n = 1$. (Here 1 is the identity symmetry.)

9. Repeat the same process in the previous two problems for a regular octahedron. (This is a polyhedron with eight equilateral triangles for faces.) (See the web page for links to web sites with templates for constructing models.)