MATHEMATICS S-152, SUMMER 2005
THE MATHEMATICS OF SYMMETRY

Outline #4 (Congruence Arithmetic)

**Reading.** Biggs, section 8.4 and chapter 13.

We define addition and multiplication of congruence classes, then explore under what circumstances congruence arithmetic does and does not lead to a group if multiplication rather than addition is chosen as the operation.

1. Identify the set of congruence classes of integers modulo $n$, denoted $\mathbb{Z}_n$. (Section 13.1). Illustrate how addition works in this set by constructing a table of addition facts for $\mathbb{Z}_4$. Show that $\mathbb{Z}_n$ is an abelian group under addition.

2. Prove that the result of addition, as specified by the rule $[x]_n + [y]_n = [x + y]_n$, does not depend on the choice of names for the classes—that using $x'$ instead of $x$ and $y'$ instead of $y$ would lead to the same equivalence class as the answer.

   A good way to lead into this is to choose a specific problem, like adding [7] to [8] in $\mathbb{Z}_{10}$, and asking everyone in the class to solve it using their own choice of elements from the classes, like 27 and $-2$. Then prove that in general everyone must get the same answer.

3. Explain how to multiply equivalence classes in $\mathbb{Z}_n$ and write out the multiplication tables for $\mathbb{Z}_3$ and $\mathbb{Z}_4$.

4. Prove that the result of multiplication, as specified by the rule $[x]_n[y]_n = [xy]_n$, does not depend on the choice of names for the classes—that using $x'$ instead of $x$ and $y'$ instead of $y$ would lead to the same equivalence class as the answer. This is the "similar proof" that Biggs mentions just before Theorem 13.2. *Note*: do not erase the multiplication table for $\mathbb{Z}_4$.

   See the pedagogical hint in topic 2.

5. Explain why $\mathbb{Z}_n$ cannot be a group under multiplication. Explain why if $n$ is not prime, even $\mathbb{Z}_n^\times$, obtained by eliminating the zero element, cannot be a group because it is not closed under multiplication. Illustrate by using the multiplication table for $\mathbb{Z}_4$.

6. Describe the Euclidean algorithm for finding the greatest common divisor of two integers (section 8.4). Illustrate the algorithm by showing that the greatest common divisor of 37 and 30 is 1. Then, using the result of this calculation, show a systematic way to determine $m$ and $n$ so that $37m + 30n = 1$.

7. Consider $\mathbb{Z}_p^\times$, where $p$ is prime. Consider an equivalence class $[a]$. By using the fact that there exist $m$ and $n$ such that $pm + na = 1$, show that $[a]$ has an inverse. For the case where $p = 37$ and $a = 30$, determine this inverse, writing it as $[b]$ where $b$ is positive and less than 37. Now summarize the proof that $\mathbb{Z}_n^\times$ is a group under multiplication if and only if $p$ is prime.

8. We know that $\mathbb{Z}_{10}$, even without the zero element, is not a group under multiplication. Show, by writing out the multiplication table, that the set consisting of [1], [3], [7] and [9] is a group under multiplication. What special property (relative to 10) do the numbers 1, 3, 7, and 9 share?

   Leave the multiplication table on the blackboard, since it is an illustration of the general result that is about to be proved.

9. Consider $\mathbb{Z}_q^\times$, where $q$ is not necessarily prime. For example, $q$ might be 10, as in the case that was just considered. Consider the set $S$ of equivalence classes $[a]$ for which the greatest common divisor of $a$ and $q$ is 1. By using the fact that there exist $m$ and $n$ such that $qm + an = 1$, show that $[a]$ has an inverse in the set $S$. Also show that if $[a]$ and $[b]$ are elements of $S$, then $[ab]$ is also in the set $S$. By running through the list of axioms for a group, conclude that the classes in the set $S$ form a group under multiplication.