MATHEMATICS 152, FALL 2003
METHODS OF DISCRETE MATHEMATICS
Outline #4 (Congruence Arithmetic and Groups)

We explore under what circumstances congruence arithmetic does and does not lead to a group if multiplication rather than addition is chosen as the operation.
Reference: Biggs, section 8.4 and chapter 13.

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

2. 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.

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

4. 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.