CS105L: Discrete Structures
I semester, 2006-07

Tutorial Sheet 5: group theory.

Instructor: Amitabha Bagchi

August 30, 2006

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

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

   Prove that G is a group under operation $\otimes$ defined as multiplication modulo n.

2. Prove the Chinese remainder theorem using the previous question. In other words prove that:

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

3. Let us define a group with two generators $\{a, b\}$ and let us say that the following relations hold $ab = b^2a$ and $ba = a^3b$.

   (a) Reduce $aba^{-1}b^{-1}$ to a string of length 1.

   (b) Reduce $bab^{-1}a^{-1}$ to a string of length 2.

   (c) Prove that $b = a^{-2}$.