MATH 113: DISCRETE STRUCTURES
HOMEWORK DUE MONDAY WEEK 12

Problem 1. Use the Fundamental Theorem of Arithmetic to prove that if p is prime, a and b are integers, and $p|ab$, then either $p|a$ or $p|b$ (or both).

Problem 2. Let p be a prime and let a be an integer $1 \leq a \leq p-1$. Consider the numbers $a, 2a, 3a, \ldots, (p-1)a$. Use the division algorithm to write

$$ia = pq_i + r_i$$

with $0 \leq r_i < p$ and integers q_i for $1 \leq i \leq p-1$.

(a) Prove that $r_i > 0$ for each i.
(b) If $r_i = r_j$, show that $p|(i-j)a$, and explain why we can then conclude that $i = j$.
(c) Prove that $\{r_1, \ldots, r_{p-1}\} = \{1, 2, \ldots, p-1\}$.