Introduction to Abstract Mathematics — Assignment 13.2

Fall 2013 — Due December 10

Exercise 1. Let $m \in \mathbb{N}$, $m \geq 2$. Prove that if $a \equiv b \pmod{m}$, then $\gcd(a, m) = \gcd(b, m)$. Thus, given an equivalence class $C \in \mathbb{Z}/m\mathbb{Z}$ it makes sense to define $\gcd(C, m) = \gcd(a, m)$, where $a \in C$ is arbitrary.

Exercise 2. Prove that $U(m) = \{C \in \mathbb{Z}/m\mathbb{Z} \mid \gcd(C, m) = 1\}$ is a group under $\times_m$.

Exercise 3. Construct the Cayley tables for $U(5)$ and $U(9)$.

Exercise 4. Prove that $\mathbb{Z}/m\mathbb{Z}$ (under $+_m$) is a cyclic group, i.e. that there is a $C \in \mathbb{Z}/m\mathbb{Z}$ so that $\langle C \rangle = \mathbb{Z}/m\mathbb{Z}$.