MATH 340 Assignment 3, Fall 2008

Michael Monagan

This assignment is to be handed in on Monday October 6th by 11:00am.
Late penalty: -20% for handing in by 9:30am Tuesday October 7th. Zero after that.

Section 1.7: Equations in $\mathbb{Z}_n$

Exercise 14.

Read Lemma 1.7.5 which says the following. If $[a]$ and $[b]$ are invertible in $\mathbb{Z}_n$ then their product $[a][b]$ is invertible in $\mathbb{Z}_n$. Rewrite the proof using [ ] notation instead of $\equiv$ notation.

Prove Corollary 1.7.6 parts (i) and (ii) on page 39.
Note that our textbook uses $(a, b) = 1$ to mean $\gcd(a, b) = 1$.

Section 1.10: Euler's ϕ-function

Exercise 3, 4.

Section 1.11: Theorem's of Euler and Fermat

Exercises 2, 3, 8.

Prove Theorem 1.11.1 (Euler's theorem) using the same approach given in class to prove Theorem 1.11.3 (Fermat's little Theorem). First prove the Lemma: if $a \in \mathbb{Z}_n^*$ then $a\mathbb{Z}_n^* = \mathbb{Z}_n^*$ where $\mathbb{Z}_n^*$ denotes the set of units in $\mathbb{Z}_n$.

Section 2.1: Basic Properties

Exercises 1, 4, 7, 10, 14, 16.
For exercise 10, use the fact that $\mathbb{Q}[\sqrt{2}]$ is a subset of the real numbers $\mathbb{R}$ which is a field, so that you don't have to prove all the field axioms.