MATH 340 Assignment 3, Fall 2017
Solutions to Additional Questions

Michael Monagan

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

Prove Lemma 1.7.9 part (i). The Lemma said
Let $a, b \in \mathbb{Z}_n$. Prove that
(i) $ax \equiv b \bmod n$ has a solution (for x) if and only if $\gcd(a, n) = 1$.

Proof ($\Rightarrow$)
We have $ax \equiv b \bmod n \Rightarrow ax - b \equiv 0 \bmod n \Rightarrow n | ax - b$.
Now let $g = \gcd(a, n)$. Now $g|n$ and $n|ax - b$ implies $g|ax - b$. But $g|a$ so $g|b$ as requried.

Proof ($\Leftarrow$) One of the students found this proof that I liked – it's better than mine.
Let $g = \gcd(a, n)$. Then there exist integers y, z such that

$$ay + nz = g$$

from the extended Euclidean algorithm. Now we are given $g|b$ so let $b = gq$ for some integer $q \in \mathbb{Z}$. Multiplying this equation by q gives

$$aqy + nqz = b.$$

Taking this modulo n gives

$$a(qy) \equiv b \mod n.$$

Thus the integer $x = qy$ satisfies the equation $ax \equiv b \mod n$.
This proof is contructive!

Section 1.11: Theorem's of Euler and Fermat

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 $\mathbb{Z}_n$.

We know that $|\mathbb{Z}_n^*| = \phi(n)$ so let $\mathbb{Z}_n^* = \{u_1, u_2, \ldots, u_{\phi(n)}\}$. Now if $a, x, y \in \mathbb{Z}_n$ satisfy $ax = ay$, since a is invertible, multiplying $ax = ay$ by a^{-1} shows that $x = y$. Thus if $x \neq y$ then $ax \neq ay$ hence

$$a\mathbb{Z}_n^* = \{au_1, au_2, \ldots, au_{\phi(n)}\} = \mathbb{Z}_n^*.$$

So

$$au_1 \times au_2 \times \cdots \times au_{\phi(n)} = u_1 \times u_2 \times \cdots \times u_{\phi(n)}.$$

Since $\mathbb{Z}_n$ is commutative the left-hand-side can be permuted to be

$$u_1 \times u_2 \times \cdots \times u_{\phi_n} \times a^{\phi(n)} = u_1 \times u_2 \times \cdots \times u_{\phi(n)}.$$

Now since the u_i are all in $\mathbb{Z}_n^*$ hence invertible, we can cancel them to give

$$a^{\phi(n)} = 1$$

in $\mathbb{Z}_n$ as required.