WORKSHEET #3 – MATH 5405
SPRING 2016

DUE: TUESDAY, 2/2/2016

We will compute inverses of some elements in some finite fields. You may work in groups.

1. Suppose that consider the ring $(\mathbb{Z}/2)[x]$. Show that the quartic polynomial $q(x) = x^4 + x + 1$ is irreducible and hence that $(\mathbb{Z}/2)[x]/q(x)$ is a field.

Hint: It is *not* enough to verify that $q(x)$ has no roots, you must *also* show it can't be factored into two quadratics.

2. Consider the polynomial $x^3 \in (\mathbb{Z}/2)[x]$. Use the Euclidean algorithm (for polynomials) to write

$$s(x) \cdot x^3 + t(x) \cdot q(x) = 1.$$

3. Use what you did in **2.** to find the multiplicative inverse of x^3 in the field $(\mathbb{Z}/2)[x]/q(x)$.

4. Now find the multiplicative inverse of $x^2 + x + 1$ in the same field.

5. How many elements does the field $(\mathbb{Z}/2)[x]/q(x)$ have? Write them all down.

6. Find at least one primitive root among those elements.