**Math 314 - Fall 2017** **Worksheet 2**

**Name 1:**____________________**Name 2:**__________________

(1) AES, one of the modern cryptosystems we will study uses $\mathbb{F}_{256} = \mathbb{F}_{2^8}$ created using the irreducible polynomial $x^8+x^4+x^3+x+1$ over $\mathbb{F}_2[x]$. We know how to add and multiply polynomials in this field, but how do we find inverses? The same as in $\mathbb{F}_p$, using Euclid's algorithm! Try this yourself to find the inverse of $x^3+x+1$ in this field.

(2) (On Back) Determine whether $x^2 \equiv 150 \pmod{1009}$ is solvable, first using Legendre symbols, then using Jacobi symbols.