Math 312
Fall 2009
Carl Miller

Proof Assignment #2

Write up solutions to **one** of the following three problems. This assignment should be done **individually**.
The due date for this assignment is Thursday, December 10th.

Problems:

1. Prove that for any two positive integers n and m,

$$\gcd\left(2^n - 1, 2^m - 1\right) = 2^{\gcd(n,m)} - 1.$$

2. Suppose that a and n are positive integers such that $\gcd(a^2, n) = \gcd(a, n)$. Prove that for some integer $m > 1$,

$$a^m \equiv a \pmod{n}.$$

3. Count the number of irreducible monic polynomials of degree 2 in $(\mathbb{Z}/13\mathbb{Z})[X]$. Prove your answer.

In your proofs, you can assume any results that are proved in Chapter 1-14 in the textbook. (However, please do not assume results that are only stated in the exercises.) You can also assume any results that were proved in class.

Guidelines & Tips: (from previous assignment)

- Make your solutions self-contained. The reader should be able to follow your proof without having to look back at the assignment sheet. (A simple way to make your solutions self-contained is to copy the problem down at the beginning of your solution.)
- If you consult any references other than the textbook, indicate that you have done so. (Example: "Sources consulted: *Algebra* by Serge Lang.") If you get help on the assignment from anyone, you should note that also.
- Use complete sentences.
- After writing out a proof, read it to yourself from beginning to end. Note any portions of the proof that are hard to read or not fully justified.
- Don't create your proofs by patching together sentences from the textbook. Proofs that are written this way are hard to read. (Also, copying from a source without proper credit is unethical.) Construct your own sentences.
- Feel free to come to office hours to discuss this assignment. I'm happy to look at a draft of a proof and give you suggestions.