EXTRA CREDIT #3– MATH 311W

DUE OCTOBER 31ST, 2012

Recall that for any integer $m > 1$, we have $\mathbb{G}_m = \{[x]_n | [x]_n \text{ is invertible}\}$. For example $\mathbb{G}_8 = \{[1]_8, [3]_8, [5]_8, [7]_8\}$. What follows is a definition.

Definition. $\mathbb{G}_m$ is called *cyclic* if there exists $x \in \mathbb{G}_m$ satisfying the following property. For every $y \in \mathbb{G}_m$, there is an exponent $k \in \mathbb{Z}$ such that $x^k = y$. In this case, x is called a *generator of* $\mathbb{G}_m$.

Now for some problems. Please *type* your solutions.

1. Prove that $\mathbb{G}_m$ is cyclic with generator x if and only if the order of x modulo m is equal to $\phi(m)$. (1 point)

2. Experiment (using a computer will help tremendously, especially if you can write a computer program / function in Maple/Mathematica/etc.) to determine for which m we have that $\mathbb{G}_m$ is cyclic. Please show your data in a table (or list or something better) to justify your conclusions. If you used software, or wrote a program, please describe the methodology and provide the source code. (up to 3 points for math + 1 point for presentation).

3. Prove your conclusion is correct (ie, $\mathbb{G}_m$ is cyclic if and only if ???). (up to 3 points for math + 1 point for presentation).