Math 42-Number Theory
Problem of the Day #9
Due Tuesday, March 8, 2011

1. For $a \in U_m$, we'll call n the *order* of a if n is the smallest natural number such that $a^n = 1$ in U_m. For example, in U_7, the order of 2 is 3 because $2^1 = 2$, $2^2 = 4$, $2^3 = 1$. Therefore, even though $2^6 = 1$ (we know this from Fermat's little theorem), $3 < 6$ so the order of 2 is 3. We call $a \in U_m$ a *generator* if every element of U_m can be expressed as a power of a–that is, if the powers of a run through all elements of U_m. For example, 3 is a generator of U_7 since $3^1 = 3$, $3^2 = 2$, $3^3 = 6$, $3^4 = 4$, $3^5 = 5$ and $3^6 = 1$.

Look at your power tables from POTD 7. What are the orders of each of the elements in U_7 and U_{15}? Do U_7 and U_{15} have generators? For $m = 4, 5, 8, 11, 16$, which U_m have a generator? Describe any patterns you see.