Math 42-Number Theory
Problem of the Day #3
Due Tuesday, February 8, 2011

We'll write U_m to mean the elements of $\mathbb{Z}_m$ that have a multiplicative inverse. So for example, $U_4 = \{1, 3\}$ since in $\mathbb{Z}_4$, 1 and 3 are invertible ($1 \cdot 1 = 1$ and $3 \cdot 3 = 9 = 1$), but 0 and 2 are not invertible.

1. List the elements of U_7, U_8, U_9, and U_{11}. When you add two elements of U_m do you necessarily get another element of U_m? When you multiply two elements of U_m do you necessarily get another element of U_m? If $a \in U_m$, is $-a$ in U_m?

2. Imagine a world with only even integers. We'll call the set of even integers $\mathbb{E}$, so in other words $\mathbb{E} = \{\ldots -6, -4, -2, 0, 2, 4, 6, \ldots\}$. In this world, what it means for a number to be prime is that it can't be factored into elements of $\mathbb{E}$. For example, even though 6 is not prime in $\mathbb{Z}$, it is prime in $\mathbb{E}$ (because 6 can't be factored into a product of even numbers). Find a number in $\mathbb{E}$ that can be factored into $\mathbb{E}$-primes in (at least) two different ways.