Math 290-Number Theory for Teachers
Problem of the Day #6
Due Wednesday, January 29, 2014

We define $\mathbb{Z}_m$ to be the set of numbers $\{0, 1, 2, \ldots, m-1\}$ with the structure of "wrapping around." Thus, $m = 0$, $m + 1 = 1$, etc. in this system. Also, $-1 = m - 1$, $-2 = m - 2$ and so on.

We write $a \equiv b \mod m$ if $a = b$ in $\mathbb{Z}_m$ and say that a and b are *congruent* modulo (or mod) m.

1. Look at $\mathbb{Z}_5$, $\mathbb{Z}_6$ and $\mathbb{Z}_7$. Find the following (or state that you can't) in $\mathbb{Z}_5$, $\mathbb{Z}_6$ and $\mathbb{Z}_7$.

$$-1,\ 100,\ 3+4,\ 3\cdot 4,\ \tfrac{1}{2},\ \tfrac{1}{5}, \sqrt{-1}$$

(Note: What is $\frac{1}{2}$? It's the number x such that $2x = 1$. What is $\sqrt{-1}$? It's the number (or numbers) x such that $x^2 = -1$.)

2. Try computing $15 \cdot 8 \mod 6$ and $(15 \mod 6) \cdot (8 \mod 6)$. What can you say about "modding out" and arithmetic operations?