# CS 165 Lab 4 Assignment

October 21, 2012

1. Our LCG spits out 8-bit random values. The first four are: DE AD BE EF. Determe the values $a, b, n$.

   Heads up: Your first homework assignment will be passed out this week. You will be required to write a program that can break a 16-bit LCG. If you write that program during the lab, you can use it to solve this problem.

Primitive Roots

- Primitive roots are those values $\alpha$ for which the smallest value $i \geq 1$ for which $\alpha^i \equiv 1 \pmod{n}$ is $i = \phi(n)$. That is, $\forall\ \alpha^i$ where $1 \leq i < \phi(n),\ \alpha^i \not\equiv 1 \pmod{n}$.
- So, we can think of $\alpha$ as being any value which, raised to successive powers, allows us to go through *every* value in the multiplicative group $\mathbb{Z}_n^*$.
- That is, if $\alpha$ is a primitive root, then for any number $g$ coprime with $n$, there exists a value $1 \leq i \leq \phi(n)$ such that $\alpha^i \equiv g \pmod{n}$.

2. For $n = 11$, $\alpha = 2$ is a primitive root. Find the value $i$ at which $2^i \equiv 9 \pmod{n}$. Finding this $i$ is known as taking the discrete logarithm.

3. For $n = 11$, find two values in $\mathbb{Z}_n^*$, other than 2, where one is a primitive root, and the other is not. Write out the set of unique values obtained by raising each to successive powers mod $n$.

4. For any modulus $n$, there are $\phi(\phi(n))$ primitive roots. List the primitive roots for $n = 11$. What does this set have in common with $\mathbb{Z}_{\phi(n)}^*$ and what is different?