Problem 25

Ryan Burmeister

February 2, 2016

Lehmer LCG Equation
$x_i \leftarrow x_{i-1} * \ a \bmod m$

When $m = 65537$, a parameter a that maximizes the period is 3. This can be proven by showing the following:

$a^d \equiv 1 \bmod m$, a is a primitive root modulo m (i.e. their greatest divisor is 1), and d is the smallest number for which the above is true.

When each of the above is true, the period will max out at a length of $m-1$. When $a = 3$, the smallest number which satisifies the equation above is 65536, and as $65536 = m - 1$, I know that I have found an ideal set of parameters of rhte Lehmer LCG.