Problem 24

Ryan Burmeister

February 2, 2016

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

When $m = 11$, the best choice for a is a primitive root modulo m as m is prime in this case. This will ensure that the period is a maximum of $m - 1$, regardless of the seed chosen.

If the seed value,is chosen to be 3, (i.e. $x_0 = 3$), and a is chosen to be 2, then the sequence generated is: $x_0 = 3$, $x_1 = 6$, $x_2 = 1$, $x_3 = 2$, $x_4 = 4$, $x_5 = 8$, $x_6 = 5$, $x_7 = 10$, $x_8 = 9$, $x_9 = 7$, $x_{10} = 3$, ...

This is a maximum length as the period is of length $10 = m - 1$, and as 10 is the first such number for $a = 2$, I know that I have found an optimal a value in 2.