# Random Number Generation Exercises

**A simple LCG.** Consider the linear congruential generator with parameters $a = 5$, $c = 0$, and $n = 32$.

(a) What is the period of $X_0 = 1$?
(b) What is the period of $X_0 = 2$?
(c) Are they any values of $X_0$ with a period greater than eight?

**Recovering parameters of an LCG.** You observe the following sequence of numbers generated using a linear congruential generator (LCG):

16, 55, 172, 11, 40, 127, 132, 147, 192, 71, 220, …

Find the values of *a*, *c*, and *n*. *Hint:* use the formula for an LCG to create a system of two linear equations and solve for *a*; once you have *a*, it's easy to solve for *c* and *n*.

**When to re-seed an AES-based PRNG.** Find NIST SP 800-90A on the NIST website. How many requests may be made to the PRNG discussed in class before it must be re-seeded? Look for the value of *reseed_interval*.

**Solving for n in BBS.** First, here is another way to think about what it means for two numbers *x* and *y* to be congruent modulo *n*. If $x \equiv y \bmod n$, then *x* and *y* differ by a multiple of *n*; in a formula, $x - y = \lambda n$ for some integer $\lambda$. Recall that in the BBS generator, the state $x_i$ is updated as follows:

$$x_{i+1} \leftarrow x_i^2 \bmod n$$

Or, in other words, $x_{i+1} \equiv x_i^2 \bmod n$, so $x_i^2 - x_{i+1} = \lambda_i n$ for some integer $\lambda_i$. Suppose a developer has implemented BBS incorrectly so that it uses the entire state $x_i$ as output rather than just the low order bit of the state. You observe the following output of the PRNG:

705387546, 24704853224, 58631086274, 73983477812, 59076648249, 51739009943, 9535414637, 9339381885

Determine the value of *n*. *Hint*: use the data to determine $\lambda_i n$ for $i = 1, 2, \ldots, 7$, then use the egcd() function to find *n*.