Name: _____

Read and take notes on the Section 16.6 Blum-Blum-Shub Generator.

Reading Questions

1. Let $p = 3$, $q = 7$, and $s_0 = 12$.
   (a) Compute the first five terms of the sequence s_i given by the recursive formula $s_{i+1} = s_i^2 \ \% \, pq$.

   (b) Compute the first five terms of the sequence b_i given by $b_i = s_i \,\%\, 2$.

2. Let $p = 7$, $q = 11$, and $s_0 = 8$.
   (a) Compute the first ten terms of the sequence s_i given by the recursive formula $s_{i+1} = s_i^2 \ \% \, pq$.

   (b) Compute the first ten terms of the sequence b_i given by $b_i = s_i \,\%\, 2$.

   (c) What is the period of this eventually periodic sequence?

3. Let $p = 5279$, $q = 7103$, and $s_0 = 27$. Given that $s_{i+1} = s_i^2 \ \% \, pq$ for $i \geq 0$, compute the first fifteen terms of the sequence b_i given by $b_i = s_i \,\%\, 2$.

4. What struck you in this reading? What is still unclear? What remaining questions do you have?