quiz 11.1

(1) Find the fixed point of the LCG given by $s_{n+1} = (47 \cdot s_n + 3) \,\%\, 101$.

(2) Find the 1000^{th} point of the LCG given by $s_{n+1} = (4 \cdot s_n + 13) \,\%\, 29$ with $s_o = 4$.

(3) Find the period of the length-eight (mod 2) LFSR with coefficients

$$(c_0, c_1, \ldots, c_7) = (0, 1, 0, 1, 0, 1, 0, 1)$$

and initial state

$$(s_0, s_1, \ldots, s_7) = (0, 0, 0, 0, 1, 1, 1, 1)$$

That is, determine the size of the loop of states that will repeat.

(4) Find the period length of the BBS pRNG with modulus $n = 43 \cdot 31$ and seed $s_o = 5$. What is the loop of pseudorandom bits?