

CSS322 – Pseudo Random Numbers

Notes

$$\begin{aligned}
 \text{LCG} : a=1 \quad c=1 \quad m=100 \\
 X_0 &= 23 \\
 X_1 &= (23+1) \bmod 100 = 24 \\
 X_2 &= 25 \\
 X_3 &= 26 \\
 X &= \{23, 24, 25, 26, \dots, 99, 0, 1, 2, \dots, 23\} \\
 &\quad \text{Period: } 100
 \end{aligned}$$

Figure 1: Linear Congruential Generator - Example 1; Lecture 07

$$\begin{aligned}
 \text{LCG} : a=7, \quad c=0, \quad m=32 \\
 X_0 &= 1 \\
 X_1 &= (7 \times 1 + 0) \bmod 32 = 7 \\
 X_2 &= (7 \times 7) \bmod 32 = 17 \\
 X_3 &= 23 \\
 X_4 &= 1 \\
 X_5 &= 7 \\
 X &= \{1, 7, 17, 23\} \\
 &\quad \text{Period} = 4
 \end{aligned}$$

Figure 2: Linear Congruential Generator - Example 2; Lecture 07

$$\begin{aligned} \text{LCG: } a=5, c=0, m=32 \\ X = \{1, 5, 25, 29, 17, 21, 9, 13\} \\ \text{Period} = 8 \end{aligned}$$

Figure 3: Linear Congruential Generator - Example 3; Lecture 07