

CSS322 – Pseudo Random Numbers and Stream Ciphers Notes

12 bits	
0111111111	1 0's
0000001111	11 1's
<u>000000</u> 1111	6 0's
6 0's	6 1's
0 1's	
0101010101	6 0's
<u>010101</u> 0101	6 1's
3 0's	
3 1's	

Figure 1: Different checks for randomness; Lecture 08

$$\text{LCG} \quad X_{n+1} = (aX_n + c) \bmod m$$

$$\text{Ex1. } a=1, c=1, m=100$$

$$\text{Seed, } X_0 = 23$$

$$X_1 = (1 \times 23 + 1) \bmod 100 = 24$$

$$X_2 = 25$$

$$X_3 = 26$$

$$X_4 = 27$$

$$X = \{23, 24, 25, 26, 27, \dots, 99, 0, 1, \dots, 22\}$$

Period = 100

$$\text{Ex2. } a=7, c=0, m=32$$

$$X_0 = 1$$

$$X_1 = (7 \times 1 + 0) \bmod 32 = 7$$

$$X_2 = (7 \times 7 + 0) \bmod 32 = 17$$

$$X_3 = (7 \times 17 + 0) \bmod 32 = 23$$

$$X_4 = (7 \times 23 + 0) \bmod 32 = 1$$

$$X = \{1, 7, 17, 23\}$$

Period = 4

$$\text{Ex3 } a=5, c=0, m=32$$

$$X = \{1, 5, 25, 29, 17, 21, 9, 13\}$$

Period = 8

$$\text{Ex4 } a=5, c=0, m=32$$

$$X = \{3, 15, 11, 23, \dots\}$$

Figure 2: Linear Congruential Generator Examples; Lecture 09