United International University

School of Science and Engineering

Course Title: Simulation and Modeling Lab

Course Code: CSI 424

Lab No: 10

**Random Number Generators**

1. **The midaquare method :**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Procedure:**   * Start with a four-digit positive integer Z0 and square it to obtain an integer with up to eight digits. [if necessary , append 0’s to the left to make it exactly eight digits] * Take the middle four digits of this eight-digit number as the next four-digit number Z1 * Place a decimal point at the left of Z1 to obtain the first U[0,1] random number,U1.   **Table of a midsquare method:**   |  |  |  |  | | --- | --- | --- | --- | | i | Zi | Ui | Zi2 | | 0 | 7182 | - | 51,581,124 | | 1 | 5811 | 0.5811 | 33,767,721 | | 2 | 7677 | 0.7677 | 58,936,329 | | 3 | 9363 | 0.9363 | 87,665,769 | | 4 | 6657 | 0.6657 | 44,315,649 | | 5 | 3156 | 0.3156 | 09,960,336 | |

1. **Linear Congruntial Generators (LCG) :**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Procedure:**   * A sequence of integers Z1 , Z2 , Z3…… is defined by the recursive formula :   Where m = the modulus, a = the multiplier, c = the increment and Z0  = the seed / starting value are nonnegative numbers.   * In order to find a random number U[0,1] then divide Zi  by m [Ui = Zi  / m]   The period of the cycle is at most m, the LCG is said to have full period. It is comforting to have full-period LCG’s since we are assured that every integer between 0 and m-1 will occur exactly once in each cycle.    **Table of LCG :**  Consider the LCG defined by m= 16,a=5,c=3 and Z0 = 7.   |  |  |  | | --- | --- | --- | | i | Zi | Ui | | 0 | 7 | - | | 1 | 6 | 0.3750 | | 2 | 1 | 0.063 | | 3 | 8 | 0.500 | | 4 | 11 | 0.688 | | 5 | 10 | 0.625 | | 6 | 5 | 0.313 | | 7 | 12 | 0.750 | | 8 | 15 | 0.938 | | 9 | 14 | 0.875 | | 10 | 9 | 0.563 | | 11 | 0 | 0.000 | | 12 | 3 | 0.188 | | 13 | 2 | 0.125 | | 14 | 13 | 0.813 | | 15 | 4 | 0.250 | | 16 | 7 | 0.438 | | 17 | 6 | 0.375 | | 18 | 1 | 0.063 | | 19 | 8 | 0.500 | |

1. **Blum Blum Shub :**

|  |
| --- |
| **Procedure :**   * Another way to generate a sequence of bits * Pick p and q to be large (like 40-digit) prime numbers, set m = pq * Xi=Xi-12 (mod m) * bi = parity of Xi (0 if even, 1 if odd)[if no of 1’s = even , set, bi = 0 and no of 1’s = odd, set bi = 1] * P=11, q=19 seed=3,window size = 4 |