Lab Report of Group 5 (Lab 2: Random number generation)

Group member list with responsibility.

|  |  |  |  |
| --- | --- | --- | --- |
| Name | Student Number | Responsibility | Contribution Percentage |
| Tao Ning | 15205926 | Paired with Su lizi to work on the deduction process. | 12.5% |
| Song Daxi | 15205922 | Worked with Sunli to complete Q2. | 12.5% |
| Raman Prasad | 15203657 |  | 12.5% |
| Su Lizi | 15205923 | Implemented the deduction process. | 12.5% |
| Wang Feihong | 15205902 |  | 12.5% |
| Wang Pin | 15205931 |  | 12.5% |
| Sun Jingqian | 15205924 |  | 12.5% |
| Sun Li | 15205925 |  | 12.5% |

b. Implementation details

We implemented the LCG algorithm in mainly three parts, which include assign the value part, algorithm method and main method.

At the first part, we defined the variable to store the value of a,c and m that used in algorithm equation. Once the user want to change the value of parameter a,c and m, the way is quit easy by changing the value of correspongidng values.

The second part, actual LCG algorithm implementation, is written exactly following the equation given by the lecture slides. The method need four parameters, which are seed, lower bound, upper bound of the random number of user that want ot generate and the number of random number the user want to generate.

The thrid part is responsible for running the main method. It allows user to enter the the number of random numbers want ot generate, lowe bound and upper bound they want to generate. In our algoritm implementation, we didn't allowed user to input seed themselves, instead we assign the seed variable by the current time. The reason for that is the seed needs to chage everytime the user want to generate to make sure the random number is reliable, due to the current time changes all the time, it is best choice for seed. The last thing part three do is print the random numbers generated by the program to the screen and output to a file.

c. Value of a, b, c and m chosen

The maximum period of LCG is M, but most of the time it will be less than M. To make LCG reach the maximum period, the following conditions should be met：

1. b and m are relatively prime
2. All the prime factors of m are divisible by a-1.
3. If m is a multiple of 4, so is a-1.
4. a,b should smaller than m
5. a and b should be positive integer.

And when we were texting it, we found It is better to choose a larger m value, which directly affects the duration of pseudo random number sequences. The larger the values of a and b, the more uniform the pseudo-random number generated. So we choose those specific values for a, b, c and m.

4. Evaluation of random.org

5. Other generators

***Xoroshiro128+*** is a very recent pseudorandom number generator which is considered to be the fastest full-period generator. It uses the uses a shift/rotate-based linear transformation. It was designed by Sebastiano Vigna in collaboration with David Blackman.

Tausworthe Generators

Extended Fibonacci Generators