Comparison of Common Linear Pseudorandom Number Generators

Schwartz, Sarah

The purpose of this project is to test the randomness of various pseudorandom linear congruential number generators. It is hypothesized that these four LCGs are not random, but that they will each display a varying degree of randomness. In order to do this, programs were written to generate sequences of numbers. These programs include RANDU, simple, rand(), and Park Miller. The results of this experiment showed that each of the random number generators failed at least one of the tests. When analyzing the number of numbers in a sequence prior to the repetition of the initial sequence it was found that there was no repetition of the original sequence with the Park Miller function, but all of the other functions did eventually repeat their initial sequence. The runs test displayed p-values of 0.4997 for RANDU, 0.4552 for rand, and 0.5874 for the Park Miller function. The overlapping sums test was performed and graphed. It demonstrated a normal distribution for RANDU and rand(), but the simple and Park Miller functions were not normally distributed. The Poker test displayed that the Park Miller function does in fact repeat although the first number never repeats. Three dimensional graphing of the Park Miller and rand() functions appeared random. However, RANDU created several vertical planes on the three-dimensional graph and is therefore not random. In conclusion, the hypothesis was partially supported by the results of this experiment. This is because the LCGs were in fact not random and they all displayed varying degrees of randomness on each test performed, but rand() outperformed the Park Miller function.