Anthony Fighter & Johnathan Stiles

COSC 374 / Winter 2016

3/20/16

Is Java’s Random Number Generator Statistically Random?

Hypothesis

Java’s random number generator is a pseudo random number generator. Furthermore, Java’s random number generator is a linear congruential generator. Since this is true, tests can be performed to determine whether the random number generator is statistically random. We predict that Java’s random number generator is not statistically random.

Experimental Description

We wrote a program in Java which allowed us to quickly generate random numbers, and find the greatest common denominator of the two random numbers. We also used a library to query random.org for true random numbers in order to compare the result with Java’s random numbers. Various seeds were tested in Java’s random number generator in order to determine whether the seed influenced the randomness of the algorithm.

Methodology

The data was analyzed using Microsoft Excel. We compared the number of trials taken with the number of pairs that were relatively prime with each other. This data was then transformed using Cesaro’s theorem to estimate pi. Both the set of Java data and the set of random.org data were analyzed using these methods.

Results

Included in the project is an excel spreadsheet with the seeds, the counts of successful relative primes out of 50 different seeds with 10,000 trials each. The resulting estimated pi values and the average pi value generated by java’s PRNG.

Conclusion

We have determined that the random numbers generated by Java’s random method may be close to true random, but are not close enough to be considered statistically random.