Phy234

PS #11/27(A)

Ziyang Gao

*5/2/2018*

*Read the first 5 pages and the “Concluding Remarks” in the article “Random Number Generators: Good Ones are Hard to Find” and answer:*

*1. What are the fundamental points that the author is making in this article?*

Many random number generators have demonstrably non-random characteristics, and a good generator is hard to find. On the other hand, porting a satisfactory generator to a wide variety of systems is not as easy as well. As far as the author has tested, the minimal standard generator, a parametric multiplicative linear congruential algorithm has withstood the test of time of its randomness and statistical independence. And it can be implemented efficiently, since numerous empirical tests of the randomness of its output has been published.

*2. List all the questions you had concerning the material in the article – anything you were confused about, didn’t understand, etc.*

I don’t really understand where the Lehmer’s algorithm came from, like what’s the mathematical rationales for it and the prove that it generates a random series of numbers. Regarding the implementation details, I don’t really understand about implementing Random in real arithmetic. So when declaring seed := temp-m\*Trunc(temp/m);