A 32-bit linear congruential random number generator with prime modulus

Hui-Chin Tang *
Kuang-Hang Hsieh
Hwapeng Chang
Department of Industrial Engineering and Management
National Kaohsiung University of Applied Sciences
Kaohsiung 80778
Taiwan, R.O.C.

Abstract

This paper explores that the different prime moduli can affect both the number of primitive root and the spectral test performance for a 32-bit *linear congruential generator* (LCG). We consider five forms of prime modulus: the Mersenne prime modulus, the largest prime modulus, the Sophie-Germain prime modulus, the twin prime modulus and the factorial prime modulus. We perform a computerized experiment that indicates significant differences exist among the number of primitive root of the five forms of prime modulus, and demonstrate that these differences can affect the performance of spectral test.

Keywords and phrases : *Linear congruential generator, Mersenne prime, Sophie-Germain prime, spectral test, full period.*

1. Introduction

A *linear congruential generator* (LCG) is defined by the following recursive formula