Eichenauer-Herrmann, Jürgen

Inverse congruential pseudorandom numbers: A tutorial. (English) Zbl 0766.65002

Int. Stat. Rev. 60, No. 2, 167-176 (1992).

This paper attempts to give a short survey of methods for generating pseudorandom numbers. It concentrates on the inversive congruential method. Three types of inversive congruential generators are distinguished with respect to a given modulus of multiplicative inversion: modulus is prime, a power of two, or an odd prime power. For these types bounds for the discrepancy (which is a measure of statistical independence used in the serial test) are calculated. It is shown that inversive congruential generators provide sequences of pseudorandom numbers with better statistical properties than classical linear congruential generators. Marsaglia's lattice test is discussed with respect to structural properties.

Reviewer: B.Mathiszik (Halle)

MSC:

65C10 Random number generation in numerical analysis
11K45 Pseudo-random numbers; Monte Carlo methods

Keywords:

discrepancy; equidistribution; inversive congruential method; lattice structure; serial test; statistical independence; uniform pseudorandom numbers

Full Text: DOI