sequence can be used (if seven sequences are required, reject every eighth term), but caution is needed when evaluating integrals by Monte Carlo methods, as this additive method should certainly not be used in more than three dimensions.

Even when p is not of the form $c^2 + 23d^2$, it is advisable to check that the period obtained is long enough. For example, $p = 151$ gives a period of $1093 = (p^2 + p + 1)/21$, and $p = 157$ gives a period of $4108 = (p^2 - 1)/6 = 26(p + 1)$, so it appears that quite possibly periods considerably shorter than p^2 are common. However, supposing the word length for integer addresses on a given (binary) machine is n, (i.e. integers $\leqslant 2^n - 1$ are allowed), then it is quite likely that there exists a prime p in the range $2^{n-1/2}$ to 2^n, satisfying all the conditions for category C of § 2 and such that $p^2 + p + 1$ is prime. For example, it was relatively easy to find $p = 2957$ and 3137 to satisfy all these conditions, and they must produce sequences of period 8 746 807 and 9 843 907 respectively, as these two numbers are themselves primes. For the Titan computer at Cambridge, $n = 20$ and since (Hardy and Wright, 1960) there are of the order of 20000 primes between 750000 and 1 048576 it appears almost certain that such a p exists, which will produce sequences with period at least 500000 million. Actually finding such a p is not an insurmountable problem; only the lack of a suitable program prevented us from finding one.

It seems reasonable to suppose that the time lost in storage and retrieval of three previously generated numbers (as opposed to one) will on many machines be more than offset by the time gained through using addition and subtraction rather than multiplication and division.

Acknowledgements

M. J. Prentice is indebted to I.C.I. Mond Division for financial support while working on this project. We are grateful to members of the Cambridge University Statistical Laboratory, especially Mr. A. D. McLaren, for suggestions and comments.

References

Downham, D. Y., and Roberts, F. D. K. (1967). Multiplicative congruential pseudo-random number generators, *Computer Journal*, Vol. 10, pp. 74–77.

Good, I. J. (1953). The Serial Test for Sampling Numbers and other Tests for Randomness, *Proc. Camb. Phil. Soc.*, Vol. 49, pp. 276–284.

Green, B. F., Smith, J. E. K., and Klem, L. (1959). Empirical Tests of an Additive Random Number Generator, *JACM*, Vol. 6, pp. 527–537.

Greenberger, M. (1965). Method in Randomness, *Comm. ACM*, Vol. 8, pp. 177–179.

Hardy, G. H., and Wright, E. M. (1960). *An Introduction to the Theory of Numbers*, Oxford University Press (4th Edition).

Naylor, T. H., Balintfy, J. L., Burdick, D. S. and King Chu (1966). *Computer Simulation Techniques*, Wiley.

Peterson, W. W. (1961). *Error Correcting Codes*, M.I.T. Press, Cambridge, Mass.

Prentice, M. J. (1967). Applied Field Notebook, Diploma in Mathematical Statistics, Cambridge.

Selmer, E. S. (1966). *Linear Recurrence Relations over Finite Fields*, Department of Mathematics, University of Bergen, Norway.

Taussky, O., and Todd, J. (1956). Generation and Testing of Pseudo-Random Numbers (in *Symposium on Monte Carlo Methods*, Ed. H. A. Meyer, Wiley, pp. 15–28).

Tocher, K. D. (1963). *The Art of Simulation*, English Universities Press.

Book Review

Lectures on Advanced Numerical Analysis, by Fritz John, 1967; 179 pages. (London: *Thomas Nelson*, 60s.)

As the author explains in a preface, this book consists essentially of the lecture notes of a course of lectures given in 1956–57, with revisions to the wording and the list of references, but no significant changes to the content to bring the material up to date. This explains, in some measure, the curious selection of numerical methods considered, no doubt also directed by the personal preferences of the author, and the historical nature of some parts of the book.

The first chapter treats the solution of linear simultaneous equations, principally by iterative and gradient methods, but includes also a discussion of matrix norms and estimates for the norm of the inverse matrix. This is followed by a chapter on the roots of polynomials largely devoted to theorems on bounds for these roots, but describing also the direct methods of Bernoulli and Graeffe, and the iterative method of Newton. These two chapters together comprise over one-third of the book.

The determination of eigenvalues of a matrix, polynomial and trigonometric approximation, and the solution of ordinary differential equations are next discussed very briefly, and the remainder of the book is devoted to the solution of partial differential equations in fair detail, especially of equations of the parabolic and hyperbolic type. Here besides the normal difference methods, the methods of Friedrich and Courant, Isaacson and Rees for the solution of hyperbolic equations as systems of first order equations are described.

Although the book cannot be recommended as a basic textbook on advanced numerical analysis today, it does contain much interesting material and would form interesting background reading to a course.

D. C. Gilles (Glasgow)