MATHEMATICS OF COMPUTATION, VOLUME 26, NUMBER 119, JULY, 1972

On the Distribution of Pseudo-Random Numbers Generated by the Linear Congruential Method

By Harald Niederreiter

Abstract. The discrepancy of sequences of pseudo-random numbers generated by the linear congruential method is estimated, thereby improving a result of Jagerman. Applications to numerical integration are mentioned.

Let m be a modulus with primitive root λ, and let y_0 be an integer in the least residue system modulo m with g.c.d.$(y_0, m) = 1$. We generate a sequence $y_0, y_1, \cdots$ of integers in the least residue system modulo m by $y_{j+1} \equiv \lambda y_j \pmod{m}$ for $j \geqq 0$. The sequence $x_0, x_1, \cdots$, defined by $x_j = y_j/m$ for $j \geqq 0$, is then a frequently employed sequence of pseudo-random numbers in the unit interval [0, 1]. Its elements x_j may also be described explicitly by $x_j = \{\lambda^j y_0/m\}$ for $j \geqq 0$, where $\{x\}$ denotes the fractional part of the real number x. The sequence $x_0, x_1, \cdots$ has period $Q = \phi(m)$, where ϕ is Euler's totient function.

For a real number α with $0 \leqq \alpha \leqq 1$, let $A(\alpha)$ be the number of elements of the sequence $x_0, x_1, \cdots, x_{Q-1}$ lying in the interval $[0, \alpha]$. We define the discrepancy $D = \sup_{0 \leqq \alpha \leqq 1} |A(\alpha)/Q - \alpha|$ which measures the deviation from the uniform distribution. Jagerman [2] has shown that $D \leqq (4/\pi)((3 \log m)/Q)^{1/2}$. His method is based on an estimate of the discrepancy in terms of certain trigonometric sums. In the present note, we shall show that a much simpler method yields a considerably sharper estimate for D (see Theorem 2). We prove also some related results.

For α from above and a positive integer k, let $A^{(k)}(\alpha)$ be the number of rationals i/k, $1 \leqq i \leqq k$, g.c.d.$(i, k) = 1$, lying in the interval $[0, \alpha]$.

THEOREM 1. *For any positive integer k, we have*

$$D^{(k)} = \sup_{0 \leqq \alpha \leqq 1} \left| \frac{A^{(k)}(\alpha)}{\phi(k)} - \alpha \right| = O(k^{\epsilon - 1}) \quad \textit{for every } \epsilon > 0.$$

Proof. For an arbitrary positive integer r, we consider the sequence of rationals $1/r, 2/r, \cdots, r/r$. There are exactly $[r\alpha]$ elements of this sequence in the interval $[0, \alpha]$. We now count these elements by a second method. We write the rationals j/r, $1 \leqq j \leqq r$, in reduced form and then count, for each positive divisor d of r, the resulting rationals with denominator d lying in $[0, \alpha]$. We thereby arrive at the identity

$$(1) \qquad [r\alpha] = \sum_{d \mid r} A^{(d)}(\alpha) \quad \text{for all } r \geqq 1 \text{ and all } \alpha,\ 0 \leqq \alpha \leqq 1.$$

Applying the Moebius inversion formula to (1), we obtain

Received January 6, 1972.
AMS 1970 *subject classifications.* Primary 65C10, 10F40; Secondary 65D30.
Key words and phrases. Pseudo-random numbers, discrepancy, numerical integration.

$$A^{(k)}(\alpha) = \sum_{d|k} \mu(d)\left[\frac{k}{d}\alpha\right] \quad \text{for all } k \geqq 1 \text{ and all } \alpha,\ 0 \leqq \alpha \leqq 1.$$

Consequently, we have, for all α with $0 \leqq \alpha \leqq 1$,

$$(2)\qquad \begin{aligned} \left|\frac{A^{(k)}(\alpha)}{\phi(k)} - \alpha\right| &= \left|\frac{1}{\phi(k)} \sum_{d|k} \mu(d)\frac{k}{d}\alpha - \frac{1}{\phi(k)} \sum_{d|k} \mu(d)\left\{\frac{k}{d}\alpha\right\} - \alpha\right| \\ &= \left|\frac{1}{\phi(k)} \sum_{d|k} \mu(d)\left\{\frac{k}{d}\alpha\right\}\right|. \end{aligned}$$

Therefore, $D^{(k)} \leqq (1/\phi(k)) \sum_{d|k} |\mu(d)| = g(k)$. Now, $g(k)$ is a multiplicative number-theoretic function. To prove that $\lim_{k\to\infty} g(k)k^{1-\epsilon} = 0$, it will therefore suffice to show that $\lim_{p^s\to\infty} g(p^s)(p^s)^{1-\epsilon} = 0$, where p^s runs through all prime powers. But $g(p^s)(p^s)^{1-\epsilon} = 2p^{-\epsilon s}(1 - 1/p)^{-1} \leqq 4p^{-\epsilon s}$, and we are done.

Let us now return to the sequence $x_0, x_1, \cdots, x_{Q-1}$. Since there is a primitive root modulo m, we must have $m = 2, 4, p^s$, or $2p^s$, where p is an odd prime and $s \geqq 1$. For $m = 2$ and 4, we readily get $D = \frac{1}{2}$ and $D = \frac{1}{4}$, respectively. For the remaining cases, we have the following estimates.

THEOREM 2. *If $m = p^s$, then $D \leqq 1/Q$. If $m = 2p^s$, then $D \leqq 2/Q$.*

Proof. We note that the sequence $x_0, x_1, \cdots, x_{Q-1}$ runs, in some order, through all the rationals i/m with $1 \leqq i \leqq m$ and g.c.d.$(i, m) = 1$. Therefore, $A(\alpha) = A^{(m)}(\alpha)$, and we can apply (2). For $m = p^s$, we get, for all α with $0 \leqq \alpha \leqq 1$,

$$\left|\frac{A(\alpha)}{Q} - \alpha\right| = \frac{1}{Q}\left|\{m\alpha\} - \left\{\frac{m}{p}\alpha\right\}\right| < \frac{1}{Q}.$$

For $m = 2p^s$, we get, for all α with $0 \leqq \alpha \leqq 1$,

$$\left|\frac{A(\alpha)}{Q} - \alpha\right| = \frac{1}{Q}\left|\{m\alpha\} - \left\{\frac{m}{2}\alpha\right\} - \left\{\frac{m}{p}\alpha\right\} + \left\{\frac{m}{2p}\alpha\right\}\right| < \frac{2}{Q}.$$

It is well known (see for instance [4]) that the discrepancy D of any sequence in [0, 1] with Q elements must satisfy $D \geqq 1/2Q$. Therefore, no substantial improvement of Theorem 2 is possible. We refer to [1] for results on the distribution of pseudo-random numbers in the case $m = 2^s$ with $s \geqq 3$ (of course, λ is then not a primitive root any more).

Theorem 2 implies two error estimates for numerical integration based on the sequence $x_0, x_1, \cdots, x_{Q-1}$. First, we apply Koksma's inequality [3] which states that, for any sequence $a_0, a_1, \cdots, a_{N-1}$ in [0, 1] with discrepancy D_N and any integrand f with bounded variation $V(f)$ on [0, 1], one has

$$\left|\frac{1}{N}\sum_{i=0}^{N-1} f(a_i) - \int_0^1 f(x)\,dx\right| \leqq V(f)D_N.$$

The notion of discrepancy is usually defined in terms of the counting functions relative to the half-open intervals $[0, \alpha,)$ $0 < \alpha \leqq 1$. But it is easily seen that this is identical with our concept of discrepancy in which we used the counting functions relative to the closed intervals $[0, \alpha]$, $0 \leqq \alpha \leqq 1$.

COROLLARY 1. *Let f be a function with bounded variation $V(f)$ in* [0, 1]. *Then*

$$\left|\frac{1}{Q}\sum_{i=0}^{Q-1} f(x_i) - \int_0^1 f(x)\,dx\right| \leqq \frac{c}{Q}V(f),$$

where $c = \frac{1}{2}$ for $m = 2$ and 4, $c = 1$ for $m = p^s$, and $c = 2$ for $m = 2p^s$.

Finally, we apply an inequality given by the present author in [4]: If $a_0, a_1, \cdots, a_{N-1}$ is a sequence in [0, 1] with discrepancy D_N and f is continuous in [0, 1] with modulus of continuity ω, then

$$\left|\frac{1}{N}\sum_{i=0}^{N-1} f(a_i) - \int_0^1 f(x)\,dx\right| \leqq \omega(D_N).$$

For the convenience of the reader, we include the short proof. We may assume without loss of generality that $0 \leqq a_0 \leqq a_1 \leqq \cdots \leqq a_{N-1} \leqq 1$. We know then from [5, Eq. (4)], [6, Theorem 1] that D_N is also given by

$$D_N = \max_{i=0,\cdots,N-1} \max\left(\left|a_i - \frac{i}{N}\right|, \left|a_i - \frac{i+1}{N}\right|\right).$$

Now,

$$\int_0^1 f(x)\,dx = \sum_{i=0}^{N-1} \int_{i/N}^{(i+1)/N} f(x)\,dx$$

$$= \sum_{i=0}^{N-1} \frac{1}{N} f(\xi_i) \text{ with } \frac{i}{N} < \xi_i < \frac{i+1}{N} \text{ for } 0 \leqq i \leqq N-1.$$

Therefore,

$$\frac{1}{N}\sum_{i=0}^{N-1} f(a_i) - \int_0^1 f(x)\,dx = \frac{1}{N}\sum_{i=0}^{N-1} (f(a_i) - f(\xi_i)).$$

But $|a_i - \xi_i| < \max(|a_i - i/N|, |a_i - (i+1)/N|) \leqq D_N$ for $0 \leqq i \leqq N-1$, hence $|f(a_i) - f(\xi_i)| \leqq \omega(D_N)$ for $0 \leqq i \leqq N-1$, and we are done.

Using the fact that ω is a nondecreasing function, we arrive at the following consequence.

COROLLARY 2. *Let f be a continuous function in* [0, 1] *with modulus of continuity ω. Then*

$$\left|\frac{1}{Q}\sum_{i=0}^{Q-1} f(x_i) - \int_0^1 f(x)\,dx\right| \leqq \omega\left(\frac{c}{Q}\right),$$

where c has the same meaning as in Corollary 1.

Department of Mathematics
University of Illinois at Urbana-Champaign
Urbana, Illinois 61801

1. U. DIETER, "Statistical interdependence of pseudo-random numbers generated by the linear congruential method," *Proc. Sympos. on Applications of Number Theory to Numerical Analysis* (Montreal, 1971), Academic Press, New York, 1972. (To appear.)

2. D. L. JAGERMAN, "Some theorems concerning pseudo-random numbers," *Math. Comp.*, v. 19, 1965, pp. 418–426. MR **32** #1877.

3. J. F. KOKSMA, "A general theorem from the theory of uniform distribution modulo 1," *Mathematica Zutphen. B*, v. 11, 1942, pp. 7–11. (Dutch) MR **7**, 370.

4. H. NIEDERREITER, "Methods for estimating discrepancy," *Proc. Sympos. on Applications of Number Theory to Numerical Analysis* (Montreal, 1971), Academic Press, New York, 1972. (To appear.)

5. H. NIEDERREITER, "Almost-arithmetic progressions and uniform distribution," *Trans. Amer. Math. Soc.*, v. 161, 1971, pp. 283–292.

6. H. NIEDERREITER, "Discrepancy and convex programming," *Ann. Mat. Pura Appl.*, 1972. (To appear.)